WESTELL

VERSALINK™ GATEWAY (MODEL 327W15-06)

USER GUIDE

Copyright © 2005 Westell, Inc

TABLE OF CONTENTS

1. PRODUCT DESCRIPTION 4
2. SAFETY INSTRUCTIONS 4
3. REGULATORY INFORMATION 5
   3.1 FCC Compliance Note 5
   3.2 Canada Certification Notice 6
4. NETWORKING REQUIREMENTS 7
5. HARDWARE FEATURES 8
   5.1 LED Indicators 8
   5.2 Cable Connectors and Switch Locations 9
   5.3 Connector Descriptions 9
6. INSTALLING THE HARDWARE 10
   6.1 Installation Requirements 10
   6.2 Before you begin 10
   6.3 Microfilters 10
   6.4 Hardware Installations 10
7. ACCESSING VERSALINK 13
   7.1 Logging on to the Network 13
   7.2 Changing the Password 14
8. CONFIGURING VERSALINK FOR INTERNET CONNECTION 16
   8.1 Confirming Your DSL Connection 16
   8.2 Setting Up an Account Profile 18
   8.3 Establishing a PPP Session 21
   8.4 Disconnecting a PPP Session 23
9. SETTING UP MACINTOSH OS X 24
10. SETTING UP ADVANCED CONFIGURATION 29
11. HOME 30
   11.1 Adding Account Profiles 30
   11.2 Editing Account Profiles 32
12. STATUS 33
   12.1 Connection Summary 33
   12.2 About 34
13. CONFIGURATION 35
   13.1 Single Static IP – Single IP Address PassThrough 35
   13.2 Service Configuration 38

13.3 Firewall Configuration....48
13.4 Wireless Configuration....52
13.5 Advanced LAN....61
13.6 Advanced WAN....75
14. SETTING UP ADVANCED SERVICE CONFIGURATION....106
14.1 Port Forwarding Ranges of Ports....107
14.2 Adding Port Forwarding Ports....107
14.3 Port Forwarding Trigger Ports....108
14.4 Adding Local Trigger Ports....109
14.5 Static NAT....110
14.6 Enabling Static NAT....111
14.7 Disabling Static NAT....113
15. MAINTENANCE....114
15.1 Backup/Restore....114
15.2 Firewall Log....115
15.3 Administrative Password....117
15.4 Remote Access....118
15.5 Update Device....120
16. TROUBLESHOOTING....125
16.1 System Self Tests....125
16.2 Diagnostic Logs....127
16.3 Statistics....130
16.4 Wireless Statistics....132
16.5 Status....134
17. NAT SERVICES....141
18. HELP....145
19. TECHNICAL SUPPORT INFORMATION....160
20. PRODUCT SPECIFICATIONS....160
21. SOFTWARE LICENSE AGREEMENT....161
22. PUBLICATION INFORMATION....163

1. PRODUCT DESCRIPTION

The Westell® VersaLink™ Gateway provides reliable, high-speed, Internet access to your existing small office phone line.

VersaLink™ is capable of data rates hundreds of times faster than a traditional analog modem. But unlike analog modems, VersaLink™ allows you to use the same phone line for simultaneous voice/fax communications and high-speed Internet access, eliminating the need for dedicated phone lines for voice and data needs. VersaLink™ supports a variety of networking interfaces such as wireless 802.11b/g, ADSL, Ethernet and the following optional features:

- ETHERNET1: Alternate WAN uplink port
- Layer w/2 QOS with VLAN tagging
- HotSpot
- Simultaneous public/private network support

Hereafter, the Westell® VersaLink™ Gateway will be referred to as "VersaLink," "Gateway," or "modem."

2. SAFETY INSTRUCTIONS

- Never install any telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch non-insulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

WARNING

Risk of electric shock. Voltages up to 140 Vdc (with reference to ground) may be present on telecommunications circuits.

3. REGULATORY INFORMATION

3.1 FCC Compliance Note

(FCC ID: CH8327WXX-6)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the Federal Communication Commission (FCC) Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment OFF and ON, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to a different circuit from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must be co-located or operating in conjunction with any other antenna or transmitter. End users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure.

Modifications made to the product, unless expressly approved by Westell Inc., could void the users' rights to operate the equipment.

PART 68 – COMPLIANCE REGISTRATION

This equipment is designated to connect to the telephone network or premises wiring using a compatible modular jack that is Part 68 compliant. An FCC compliant telephone cord and modular plug is provided with the equipment. See the Installation Information section of this User Guide for details.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instruction for details.

If this terminal equipment (Model 327W) causes harm to the telephone network, the telephone company may request you to disconnect the equipment until the problem is resolved. The telephone company will notify you in advance if temporary discontinuance of service is required. If advance notification is not practical, the telephone company will notify you as soon as possible. You will be advised of your right to file a complaint with the FCC if you believe such action is necessary. If you experience trouble with this equipment (Model 327W), do not try to repair the equipment yourself. The equipment cannot be repaired in the field. Contact your Internet service provider (ISP) or contact the original provider of your DSL equipment.

The telephone company may make changes to their facilities, equipment, operations, or procedures that could affect the operation of this equipment. If this happens, the telephone company will provide advance notice in order for you to make the modifications necessary to maintain uninterrupted service.

If your home has specially wired alarm equipment connected to the telephone line, ensure that the installation of this equipment (Model 327W) does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

This equipment cannot be used on public coin phone service provided by the telephone company. Connection of this equipment to party line service is subject to state tariffs.

3.2 Canada Certification Notice

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operations and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The department does not guarantee the equipment will operate to the user's satisfaction.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specification. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specification were met. It does not imply that Industry Canada approved the equipment. The Ringer Equivalence Number (REN) is 0.0. The Ringer Equivalence Number that is assigned to each piece of terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local Telecommunication Company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Connection to a party line service is subject to state tariffs. Contact the state public utility commission, public service commission, or corporation commission for information.

If your home has specially wired alarm equipment connected to the telephone line, ensure that the installation of this equipment (Model 327W) does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

If you experience trouble with this equipment (Model 327W), do not try to repair the equipment yourself. The equipment cannot be repaired in the field and must be returned to the manufacturer. Repairs to certified equipment should be coordinated by a representative, and designated by the supplier. Refer to section 19 in this User Guide for further details.

The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

Users should ensure, for their own protection, that the electrical ground connections of the power utility, telephone lines, and internal, metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

⚠ CAUTION ⚠

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

4. NETWORKING REQUIREMENTS

The following system specifications are required for optimum performance of the VersaLink™ via 10/100 Base-T or Wireless installations.

CONNECTION TYPE	MINIMUM SYSTEM REQUIREMENTS
ETHERNET	• Pentium® or equivalent class or higher machines • Microsoft® Windows® (98 SE, ME, 2000, NT 4.0, or XP) Macintosh® OS X, or Linux installed • 64 MB RAM (128 MB recommended) • 10 MB of free hard drive space • TCP/IP Protocol stack installed • 10/100 Base-T Network Interface Card (NIC) • Computer Operating System CD-ROM on hand
WIRELESS IEEE 802.11g	• Pentium® or equivalent class or higher machines • Microsoft® Windows® (98 SE, ME, 2000, or XP) or Macintosh® OS X installed • Computer Operating System CD-ROM on hand • Internet Explorer 4.x or Netscape Navigator 4.x or higher • 64 MB RAM (128 MB recommended) • 10 MB of free hard drive space • An available IEEE 802.11b/g PC adapter

5. HARDWARE FEATURES

5.1 LED Indicators

This section explains the LED States and Descriptions. LED indicators are used to verify the unit's operation and status.

LED States and Descriptions

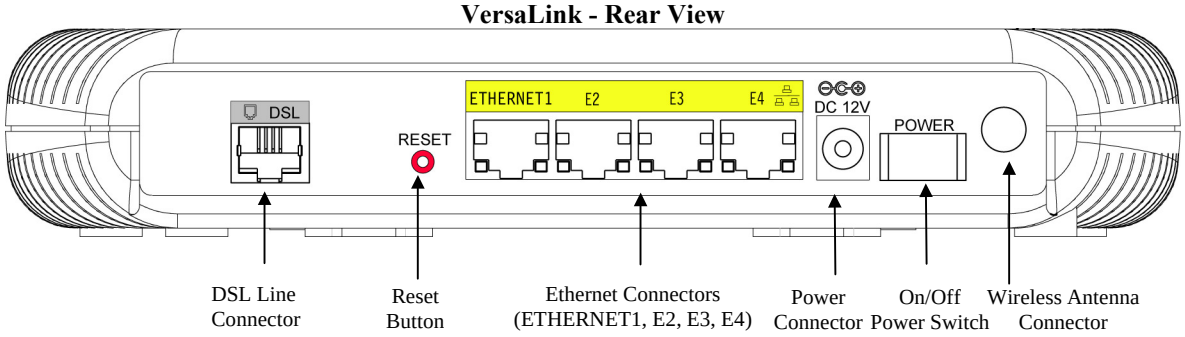
LED	State	Description
POWER	**Solid Green**	Modem power is ON.
	OFF	Modem power is OFF.
	Solid Red	POST (Power On Self Test), Failure (not bootable) or Device Malfunction. Note: The Power LED should be red no longer than two seconds after the power on self test passes.
E1, E2, E3, E4 (Ethernet LAN)	**Solid Green**	Powered device is connected to the associated port (includes devices with wake-on LAN capability where slight voltage is supplied to an Ethernet connection). Note: When using the optional uplink port (E1), Ethernet LAN connection is limited to E2, E3, and E4.
	Flashing Green	10/100 Base-T LAN activity is present (traffic in either direction)
	OFF	Modem power is OFF, no cable or no powered device is connected to the associated port.
WIRELESS	**Solid Green**	Link Established.
	Flashing Green	Wireless LAN activity is present (traffic in either direction).
	OFF	Modem power is OFF or No Link.
DSL	**Solid Green**	Good DSL sync.
	Flashing Green	DSL attempting to sync.
	OFF	Modem power is OFF.
INTERNET	**Solid Green**	Internet link established.
	Flashing Green	IP connection established and IP Traffic is passing through device (in either direction). Note: If the IP or PPP session is dropped due to an idle timeout, the light will remain solid green, if an ADSL connection is still present. If the session is dropped for any other reason, the light is turned OFF. The light will turn red when it attempts to reconnect and DHCP or PPP fails).
	Solid Red	Device attempted to become IP connected and failed (no DHCP response, no PPP response, PPP authentication failed, no IP address from IPCP, etc.).
	OFF	Modem power is OFF, Modem is in Bridge Mode, or the connection is not present.
NOTE: Safe Boot is reflected when the Power and Internet LED's are both red and all other LED's are off.		

5.2 Cable Connectors and Switch Locations

- DSL connector (RJ-11)
- Reset button
- (4) Ethernet connector (RJ-45) with optional uplink port (ETHERNET1)
  (Note: When using optional uplink port, ETHERNET1, Ethernet LAN is limited to E2, E3, and E4.)
- Power connector (DC 12V) barrel
- Power ON/OFF switch
- Wireless IEEE 802.11b/g SMA connector and antenna

Note: When VersaLink is configured for uplink mode (that is, you have selected **ETHERNET PORT 1** via the WAN configuration settings), the port labeled **ETHERNET1** on the rear panel functions as a WAN uplink port and Ethernet LAN connection is limited to ports E2, E3, and E4. However, when VersaLink is configured for **DSLATM PORT** via the WAN configuration settings, all four Ethernet ports on the rear panel may be used for Ethernet LAN connection. In **DSLATM PORT** mode, VersaLink will use DSL and wireless connection only.

VersaLink - Rear View



5.3 Connector Descriptions

The following chart displays the connector types.

SYMBOL	NAME	TYPE	FUNCTION
	DSL LINE	6-pin RJ-11 modular jack	Connects to an ADSL-equipped telephone jack or DSL connection of a POTS splitter.
	ETHERNET	8-pin (RJ-45) modular jack	10/100 Base-T Ethernet connection to PC or Hub.
DC 12V	POWER	Barrel connector	Connection to DC (12V) power connector.
Wireless	ANTENNA	SMA connector and antenna	Connects to wireless IEEE 802.11b/g device.

6. INSTALLING THE HARDWARE

6.1 Installation Requirements

To install VersaLink™, you will need the following:

- A Network Interface Card (NIC) installed in your PC, or
- An IEEE 802.11b/g adapter
- A DSL line

IMPORTANT: Please wait until you have received notification from your Internet service provider (ISP) that your DSL line has been activated before installing your VersaLink and software.

6.2 Before you begin

Make sure that your kit contains the following items:

- Westell VersaLink™ Gateway
- Power Supply
- RJ-45 Ethernet cable (straight-through) (yellow)
- RJ-11 Phone cable (blue)
- SMA Antenna

6.3 Microfilters

ADSL signals must be blocked from reaching each telephone, answering machine, fax machine, computer modem or any similar conventional device. Failure to do so may degrade telephone voice quality and ADSL performance. Install a microfilter if you desire to use the DSL-equipped line jack for telephone, answering machine, fax machine or other telephone device connections. Microfilter installation requires no tools or telephone rewiring. Just unplug the telephone device from the baseboard or wall mount and snap in a microfilter, next snap in the telephone device. You can purchase microfilters from your local electronics retailer, or contact the original provider of your DSL equipment.

6.4 Hardware Installations

The following instructions explain how to install VersaLink for Ethernet only and Wireless only connections. However, VersaLink supports simultaneous use of 10/100 Base-T Ethernet and Wireless configurations. If you desire to use Ethernet and Wireless simultaneously, follow the instructions provided in both sections 6.4.1 and 6.4.2.

IMPORTANT: If you are using VersaLink in conjunction with an Ethernet Hub or Switch, refer to the manufacturer's instructions for proper installation and configuration. When using a Microfilter, be certain that the DSL phone cable is connected to the "DSL/HPN" non-filtered jack. **Westell recommends the use of a surge suppressor to protect equipment attached to the power supply.** Additional Ethernet cables may be required depending on the installation method you are using. Ethernet cables can be purchased at your local computer hardware retailer.

6.4.1 Connecting PCs via 10/100 Base-T Ethernet

IMPORTANT: Before you connect via 10/100 Base-T, you must have an available Ethernet card installed in your computer. If your Ethernet card does not auto-negotiate, you must set it to half duplex. Refer to the Ethernet card manufacturer's instructions for installing and configuring your Ethernet card.

1. Connect the DSL phone cable from the connector marked on the rear panel of VersaLink to the DSL-equipped telephone line jack on the wall. **IMPORTANT:** Do not use a DSL filter on this connection. You must use the phone cord that was provided with the kit.
2. Connect the yellow Ethernet cable from any one of the Ethernet jacks marked on the rear panel of VersaLink to the Ethernet port on your computer. **Repeat this step to connect up to three additional PCs to VersaLink.**
3. Connect the power supply cord to the power connector marked **DC 12V** on the rear panel of VersaLink. Plug the other end of the power supply into a wall socket, and then turn on the power switch (if it is not already turned on).

   NOTE: You may connect to any of the four Ethernet jacks on the rear panel of your VersaLink as they serve as an Ethernet switch. However, when using the optional uplink port (ETHERNET1), Ethernet LAN connection is limited to ports E2, E3, and E4.

4. Check to see if the DSL LED is solid green. If the DSL LED is solid green, VersaLink is functioning properly.
5. Check to see if the Ethernet LED is solid green. Solid green indicates that the Ethernet connection is functioning properly.
6. Check to see if the Internet LED is solid green. Solid green indicates that the Internet link has been established.

Congratulations! You have completed the Ethernet hardware installation. Proceed to section 7, "Accessing VersaLink," to access VersaLink's web pages.

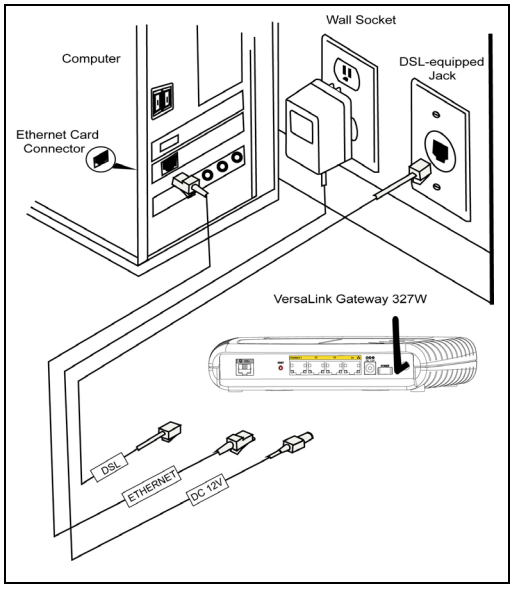


Figure 1. Connection via 10/100 Base-T Ethernet

6.4.2 Connecting PCs via Wireless

IMPORTANT: If you are connecting to VersaLink via a wireless network adapter, the SSID must be the same for both VersaLink and your PC's wireless network adapter. The default SSID for VersaLink is the serial number of the unit (located below the bar code on the bottom of the unit and also on the Westell shipping carton). Before you begin your account setup and configuration procedures, locate and run the utility software provided with your PC's wireless network adapter and enter the SSID value. Your PC's wireless network adapter must be configured with the SSID (in order to communicate with VersaLink). Later, for privacy, you can change the SSID by following the procedures outlined in section 13.4, "Wireless Configuration."

IMPORTANT: Client PCs can use any Wireless Fidelity (Wi-Fi) 802.11b/g certified card to communicate with VersaLink; however, the Wireless card and VersaLink must use the same security code type. **If you use WPA-PSK or WEP wireless security, you must configure your PC's wireless adapter for the security code that you use.**

To network VersaLink to additional PCs in your home or office using wireless, you will need to confirm the following:

1. Ensure that an 802.11b/g wireless network adapter has been installed in each PC on your wireless network.
2. Install the appropriate drivers for your Wireless IEEE802.11b or IEEE802.11g adapter.
3. Make sure the SMA antenna connector is on tight, then orient the antenna to the proper configuration.
4. Connect the DSL phone cable from the connector marked on the rear panel of VersaLink to the DSL-equipped telephone line jack on the wall. **IMPORTANT:** Do not use a DSL filter on this connection. You must use the phone cord that was provided with the VersaLink kit.
5. Connect the power supply cord to the power connector marked **DC 12V** on the rear panel of VersaLink. Plug the other end of the power supply into a wall socket, and then turn on the power switch (if it is not already on).
6. Check to see if the DSL LED is solid Green. Solid green indicates that VersaLink is functioning properly.
7. Check to see if VersaLink's Wireless LED is solid green. Solid green indicates that the Wireless interface is functioning properly.
8. Check to see if the Internet LED is solid green. Solid green indicates that the Internet link has been established.

Congratulations! You have completed the Wireless installation. Proceed to section 7, "Accessing VersaLink," to access VersaLink's web pages.

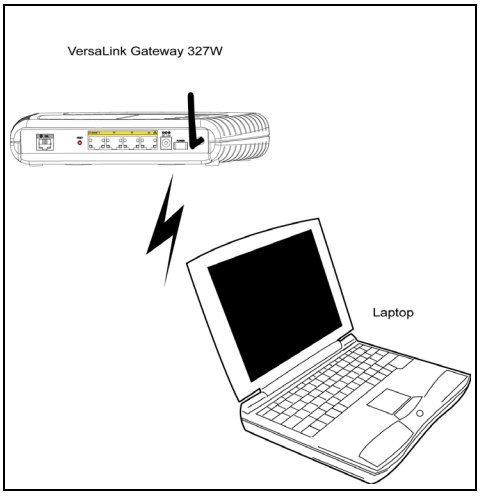


Figure 2. Connection via Wireless

7. ACCESSING VERSALINK

7.1 Logging on to the Network

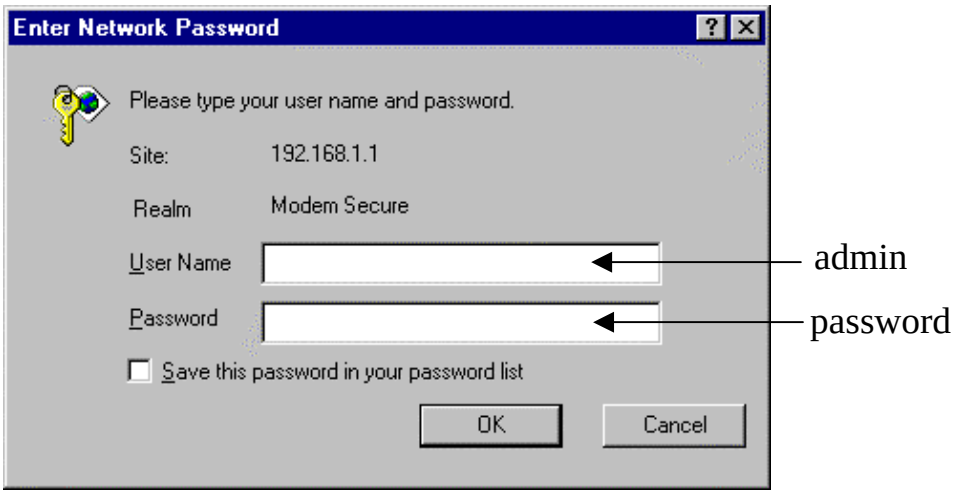
This section explains the network logon procedures for your VersaLink. This procedure should be used any time you need to access or make changes to your VersaLink or Firewall settings.

IMPORTANT: VersaLink has the capability of automatically sensing protocol type (DHCP or PPPoE). This process is designed to start after you have connected your VersaLink. To access VersaLink, your PC must be configured for DHCP. Refer to your Windows help screen for information on configuring your computer for DHCP. Click on **Start**, then **Help** to access the Windows help screen.

Start your web browser and type the following IP address in the browser's address bar:

http://192.168.1.1

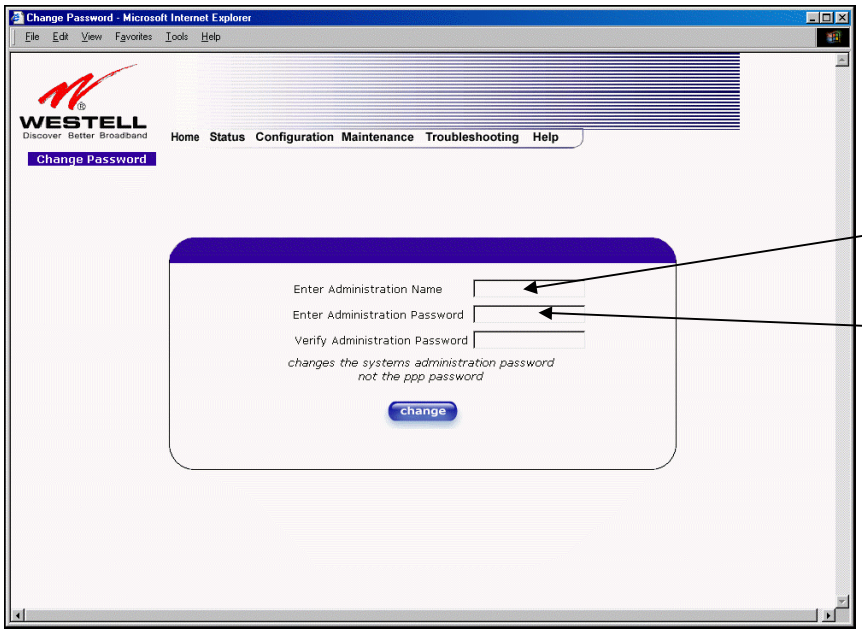
After you type the IP address, press 'Enter' on your keyboard. The following screen will be displayed. Type the default user name (which is **admin**) and the default password (which is **password**) in the fields provided. Click **OK.**



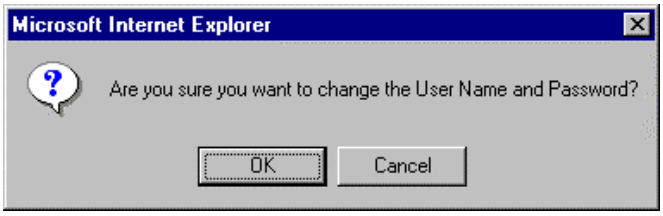
7.2 Changing the Password

After VersaLink has been reset, the following **Change Password** screen will be displayed. This screen allows you to change the default administration name and password to the values of your choice. The password change is required to continue your network logon. Enter your **Administration** name and your **Password** in the fields provided, and then click **change.**

IMPORTANT: The **Change Password** screen allows you to use **admin** as your **administration name** (your administration name can match your user name). However, this screen does not allow you to use **"password"** as your **administration password**. You must enter a different password in order for this screen to take effect. If you enter **password** in the fields labeled **Enter Administration Password** and **Verify Administration Password**, this screen will not continue the logon. **Once you decide on an administration name and a password, please record them for future reference.**


Change Password - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Change Password
Enter Administration Name
Enter Administration Password
Verify Administration Password
changes the systems administration password
not the ppp password
change
Type **admin** or the name of your choice.
Type a new password. (Do not type the word **password** here.)

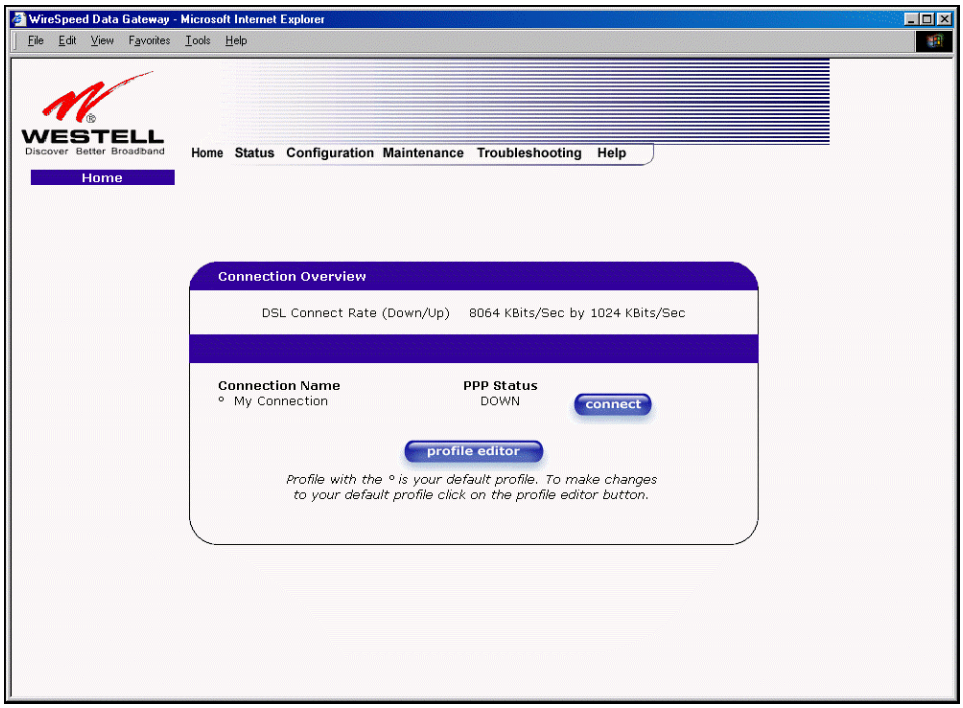
If you clicked on **change,** the following pop-up screen will be displayed. Click **OK.**



If you clicked **OK** in the preceding pop-up screen, the following screen will be displayed. Now proceed to section 8 to configure VersaLink for Internet connection.

NOTE: If VersaLink has established a DSL connection and if you are connecting via DHCP, you may now browse the Internet. Follow the instructions provided by your Internet service provider. If you are connecting via PPP, proceed to section 8 to configure VersaLink for Internet connection.

In this screen, VersaLink has established a DSL connection, and the connection rates are displayed. DHCP customers may now browse the Internet. PPP customers should proceed to section 8 for instructions on configuring VersaLink for Internet connection.


WireSpeed Data Gateway - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Home
Connection Overview
DSL Connect Rate (Down/Up) 8064 KBits/Sec by 1024 KBits/Sec
Connection Name
° My Connection
PPP Status
DOWN
connect
profile editor
Profile with the ° is your default profile. To make changes to your default profile click on the profile editor button.

8. CONFIGURING VERSALINK FOR INTERNET CONNECTION

To browse the Internet using your VersaLink Gateway, you must confirm your DSL connection, set up your account profile, and establish a PPP session with your Internet service provider (ISP).

8.1 Confirming Your DSL Connection

After you have logged on to VersaLink and changed your administrator password (as explained in section 7), the following screen will displayed.

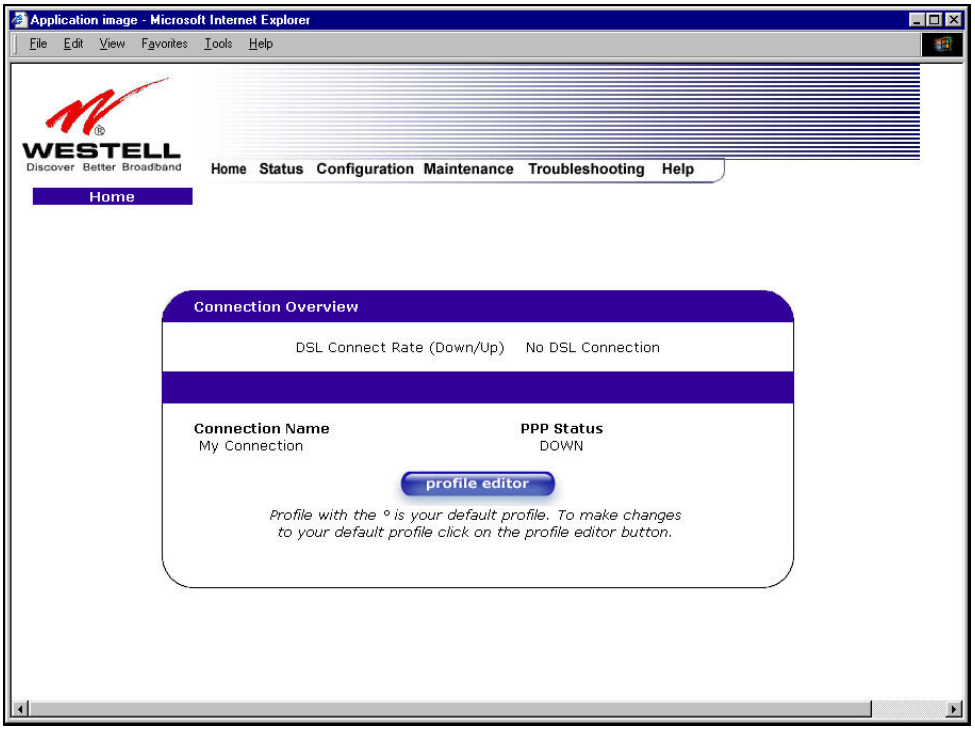
IMPORTANT: You must have active DSL service before VersaLink can synchronize with your ISP's equipment.

To determine if VersaLink has established a DSL sync

- View the DSL Connection Rate in the **Connection Overview** section. If the status reads **No DSL Connection**, you do not have a DSL sync. (If this field displays numeric values, a DSL sync has been established. Please wait a brief moment for the VersaLink to report these values.)
- Check to see if VersaLink's **DSL** LED is solid green. Solid green indicates that VersaLink's DSL connection has been established. (The **DSL** LED may flash while the connection is being established.)

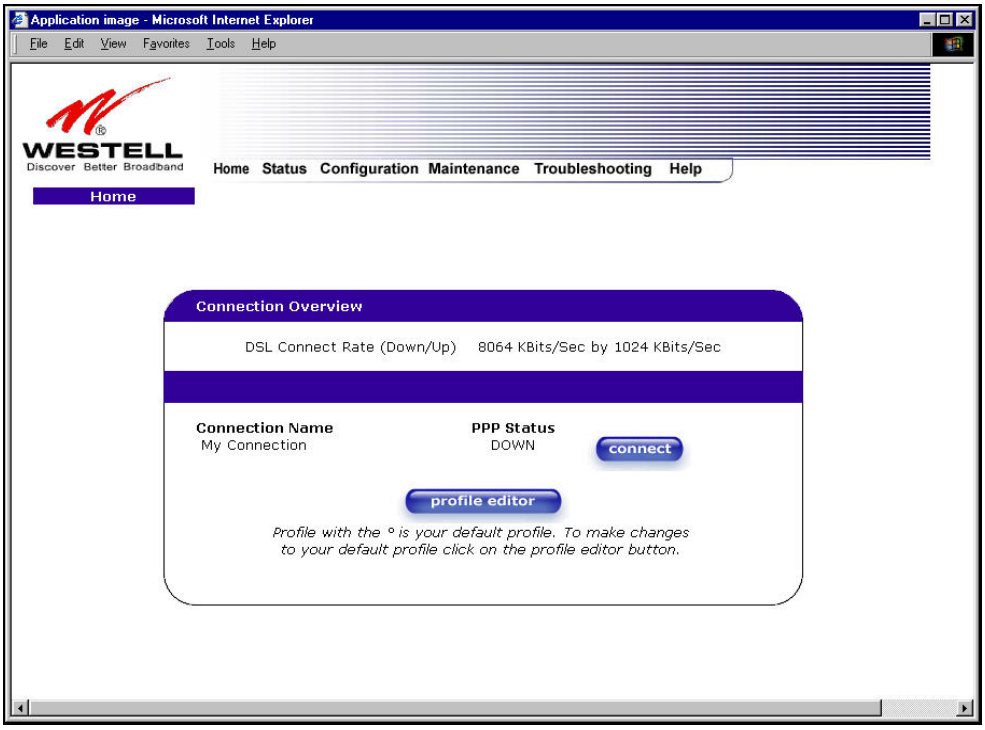
If you do not have a DSL sync, first check your physical connections (if needed, refer to section 6, Installing the Hardware). Then, if the problem persists, contact your ISP for further instructions.

NOTE: If no DSL sync is established, the **connection** button in this screen will not be displayed.


Application image - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Home
Connection Overview
DSL Connect Rate (Down/Up) No DSL Connection
Connection Name
My Connection
PPP Status
DOWN
profile editor
Profile with the ° is your default profile. To make changes to your default profile click on the profile editor button.

The following screen shows the DSL connection rate with values that indicate a successful DSL sync has been established. The connection rate values represent the transmission speed of your DSL line. (VersaLink may take time to report these values.) After you have confirmed your DSL connection, click the **Connect** button to set up your account profile.

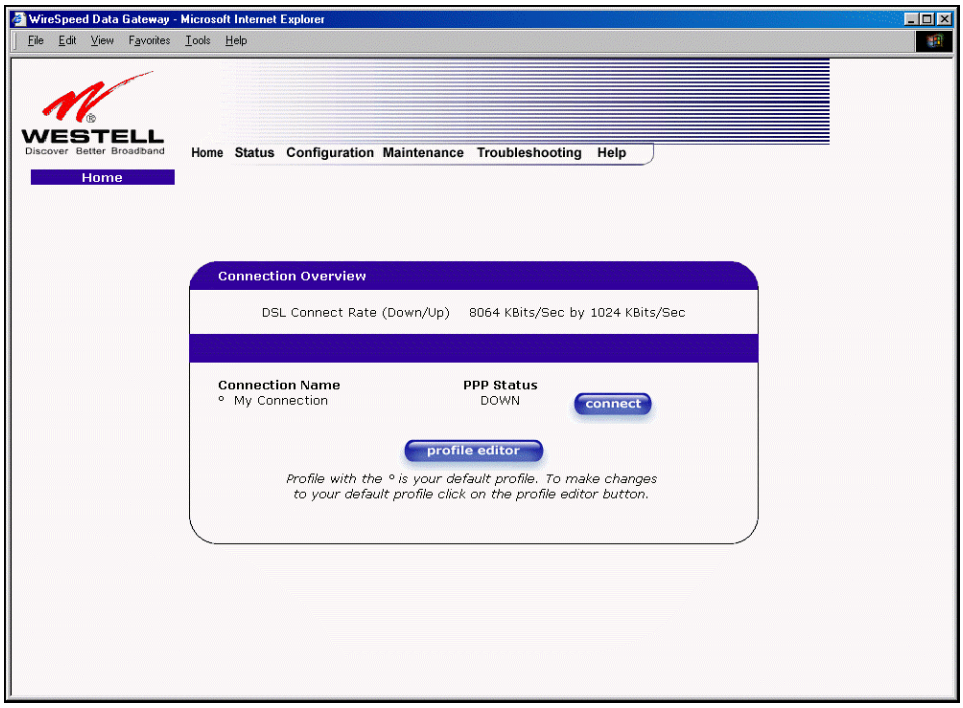
NOTE: VersaLink will handle transmission rates up to 8 Mbps.


Application image - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Home
Connection Overview
DSL Connect Rate (Down/Up) 8064 KBits/Sec by 1024 KBits/Sec
Connection Name
My Connection
PPP Status
DOWN
connect
profile editor
Profile with the ° is your default profile. To make changes to your default profile click on the profile editor button.

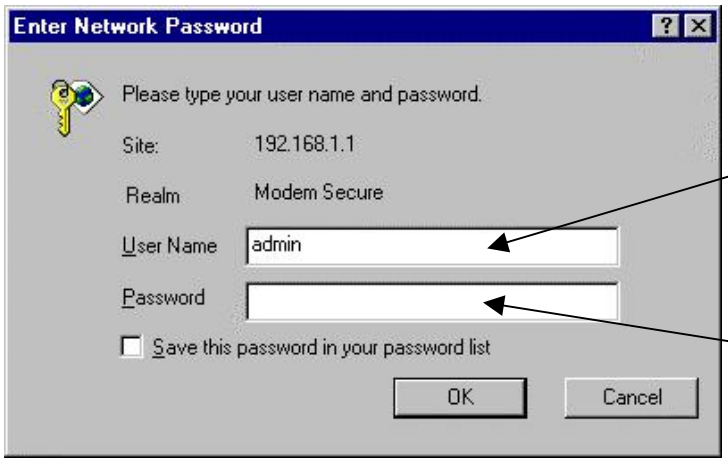
8.2 Setting Up an Account Profile

Your account profile is used to identify you to your ISP. To begin your account setup, click **profile editor.**

NOTE: Before you set up your account profile, obtain your **Account ID**, **Account Password** from your ISP. You will use this information when you set up your account parameters.


WireSpeed Data Gateway - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Home
Connection Overview
DSL Connect Rate (Down/Up) 8064 KBits/Sec by 1024 KBits/Sec
Connection Name
° My Connection
PPP Status
DOWN
connect
profile editor
Profile with the ° is your default profile. To make changes to your default profile click on the profile editor button.

If you clicked **profile editor** in the preceding screen, the following screen will be displyed. Enter the **User name** and **Password** that you used in the **Change Password** screen in section 7.2, and then click **OK** to continue.

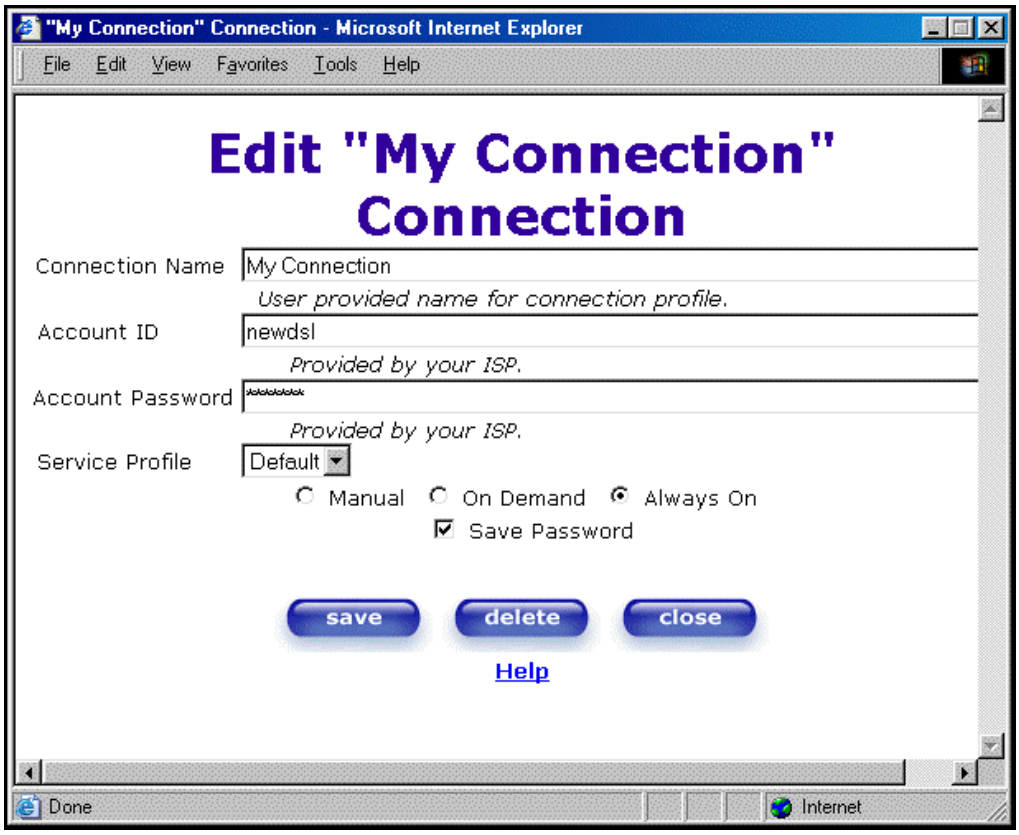


Enter the name you used in the **Change Password** screen.

Enter the password you used in the **Change Password** screen.

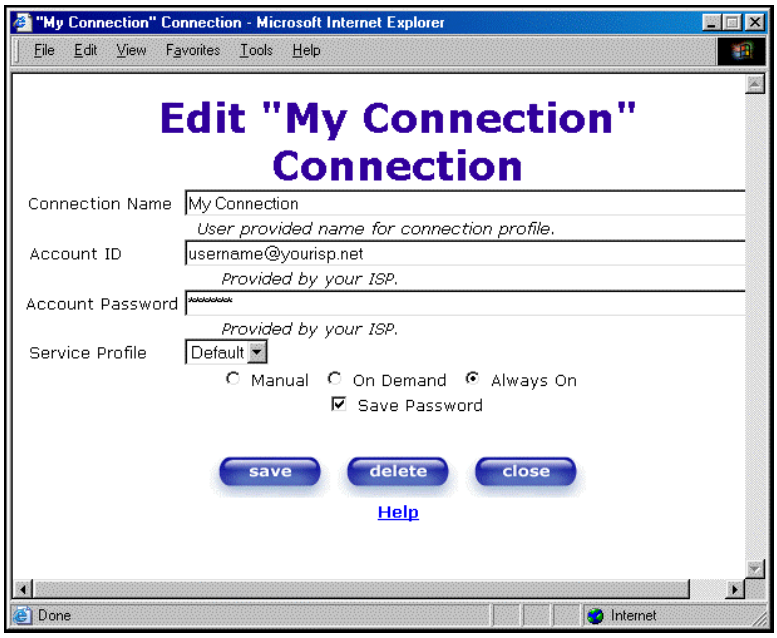
If you clicked **OK,** the folowing screen will be displayed. The screen allows you to set up your account profile. The following account parameters are required for your Internet connection:

- **Connection Name**-the Connection Name is a word or phrase that you use to identify your account. (You may enter up 64 characters in this field.)
- **Account ID**-the Account ID is provided by your ISP. (You may enter up 255 characters in this field.)
- **Account Password-**the Account Password is provided by your ISP. (You may enter up 255 characters in this field.)

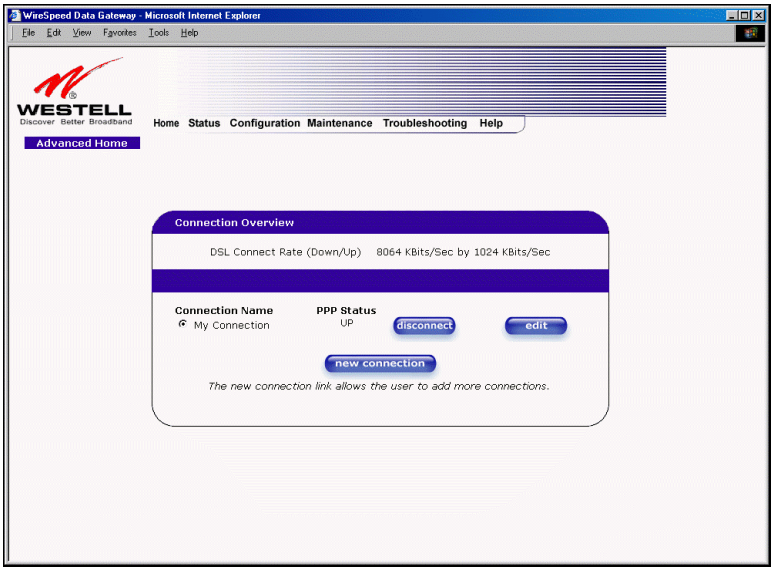


Type your account parameters in the fields provided. Next, select the type of connection setting (Manual, On Demand, Always On) that you want to use for your default service profile. Then, click **save** to save the settings.

- **Manual:** Select this option if you want to manually establish your PPP session.
- **On Demand:** Select this option if you want VersaLink to automatically re-establish your PPP session on demand anytime your PC requests Internet activity (for example, browsing the Internet, email, etc.). When you have traffic, this feature may cause a delay.
- **Always On:** Select this option if you want VersaLink to automatically establish a PPP session when you log on or if the PPP session goes down.



If you clicked **save,** the following **Connection Overview** screen will be displayed. Now proceed to section 8.3 to establish your PPP session.

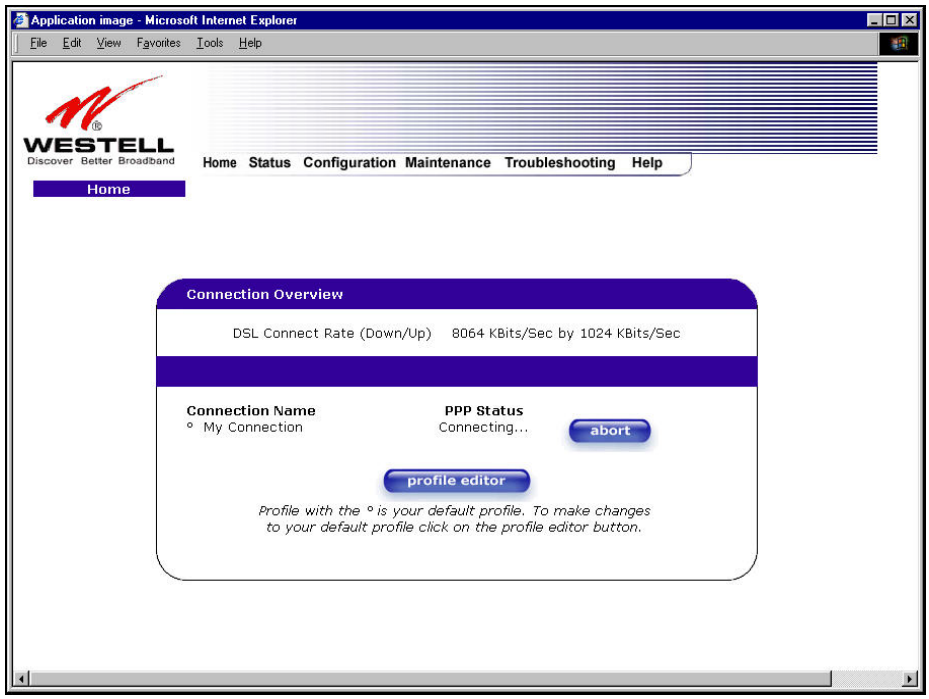


8.3 Establishing a PPP Session

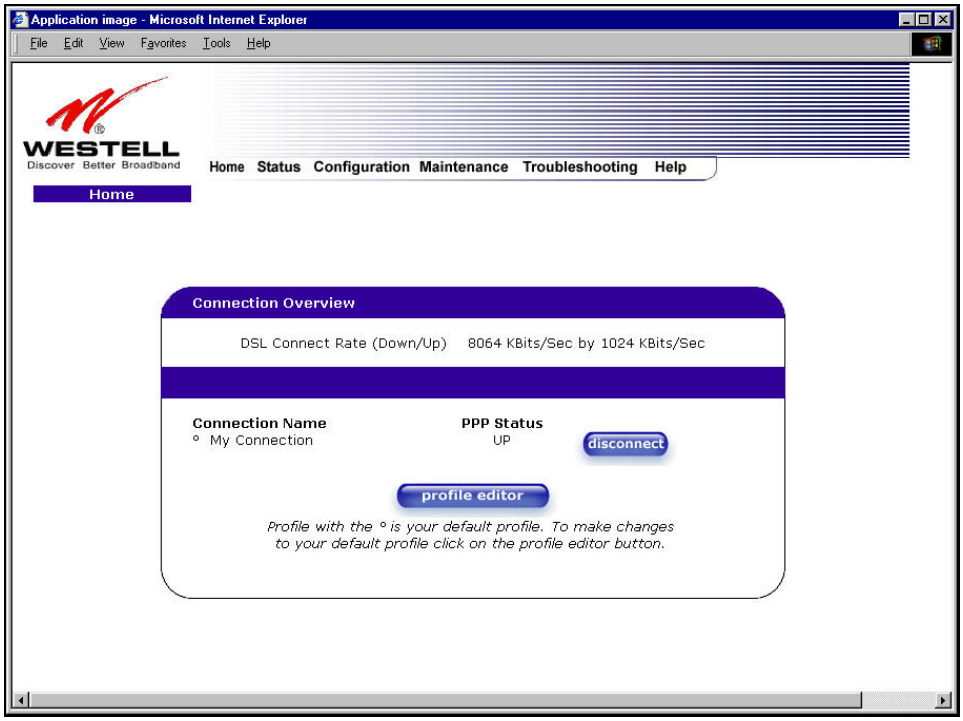
After you have set up your connection profile and clicked **save,** view the **PPP Status** field at the **Connection Overview** screen. If **PPP Status** displays **DOWN,** you do not have a PPP session. Click the **Connect** button to establish a PPP session.

NOTE: Whenever **PPP Status** displays **DOWN,** you do not have a PPP session established. If your Gateway's connection setting is set to "Always On" or "On Demand," after a brief delay, the PPP session will be established automatically and the PPP Status will display **UP.** If the connection setting is set to "Manual," you must click on the **Connect** button to establish a PPP session. Once the PPP session has been established (PPP Status displays **UP**), you may proceed with your Gateway's configuration. Section 11.2 provides instructions on editing the connection settings. (Refer to the 'Edit My Connection' screen.) VersaLink's factory default connection setting is "Always On."

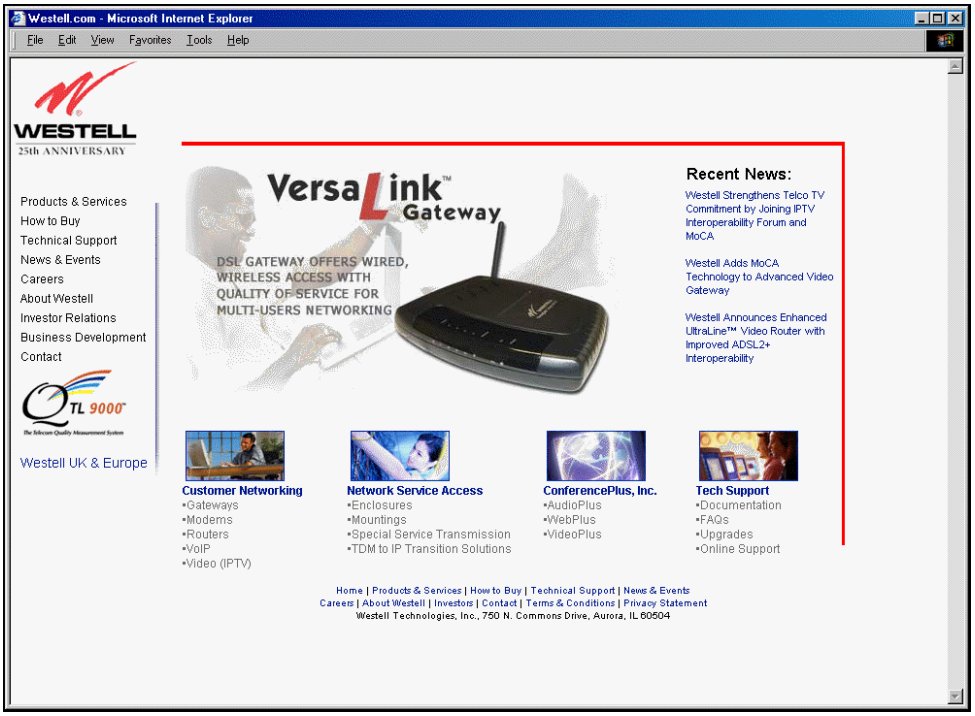
If you click the **Connect** button, the following screen will appear briefly. The **PPP Status** in the **Connection Overview** window allows you to view the state of your PPP connection. When the **PPP Status** displays **Connecting…**, this means that you are establishing a PPP session.


Application image - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Home
Connection Overview
DSL Connect Rate (Down/Up) 8064 KBits/Sec by 1024 KBits/Sec
Connection Name
° My Connection
PPP Status
Connecting...
abort
profile editor
Profile with the ° is your default profile. To make changes to your default profile click on the profile editor button.

After a PPP session has been established, the **PPP Status** will display **UP**. Congratulations! You may now browse the Internet.


Application image - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Home
Connection Overview
DSL Connect Rate (Down/Up) 8064 KBits/Sec by 1024 KBits/Sec
Connection Name
° My Connection
PPP Status
UP
disconnect
profile editor
Profile with the ° is your default profile. To make changes to your default profile click on the profile editor button.

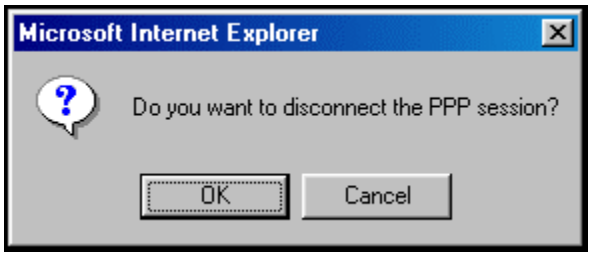
For example, if you want to visit Westell's home page, type **http://www.westell.com** in your browser's address window, and then press 'Enter' on your keyboard.



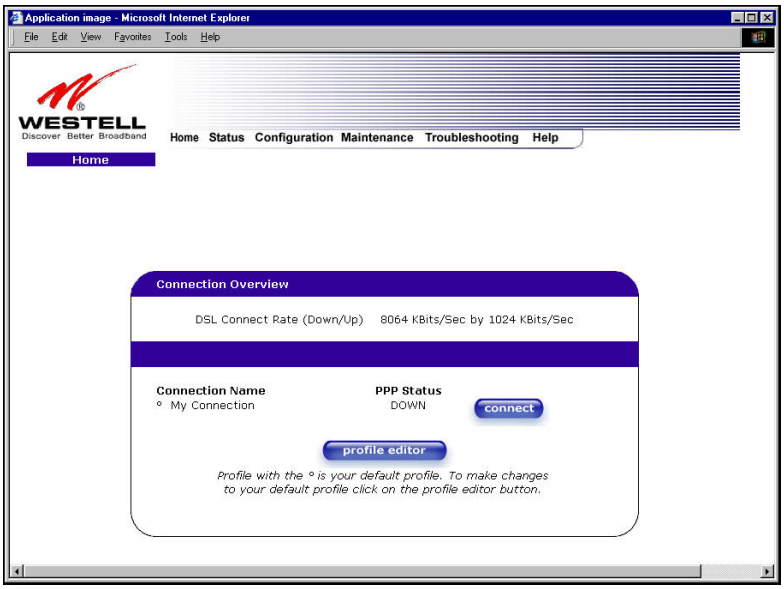
8.4 Disconnecting a PPP Session

If you have finished browsing the Internet and want to disconnect from your service provider, click the **Disconnect** button in the **Connection Overview** screen. The following pop-up screen will appear. Click **OK** to disconnect the PPP session.

Warning: If you disconnect the PPP session, this will disconnect VersaLink from the Internet, and all users will be disconnected until the PPP session is re-established.



If you clicked the **Disconnect** button in the preceding **Connection Overview** screen, the **PPP Status** should display **DOWN**. This means that you no longer have a PPP session. However, your DSL session will not be affected. When you are ready to end your DSL session, simply turn off VersaLink via the power switch on VersaLink's rear panel.


Application image - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Home
Connection Overview
DSL Connect Rate (Down/Up) 8064 KBits/Sec by 1024 KBits/Sec
Connection Name
° My Connection
PPP Status
DOWN
connect
profile editor
Profile with the ° is your default profile. To make changes to your default profile click on the profile editor button.

When you are ready to establish a PPP session, click the **connect** button. (If you have previously turned off VersaLink, first turn on VersaLink, and then log on to your account profile to establish a PPP session.)

NOTE: When you are ready to exit VersaLink's interface, click on the **X** (close) in the upper-right corner of the window. Closing the window will not affect your PPP Status (your PPP session will not be disconnected). You must click on the **disconnect** button to disconnect your PPP session. When you are ready to restore this interface, launch your Internet browser and type **http://192.168.1.1/** in the browser's address bar, and press 'Enter' on your keyboard.

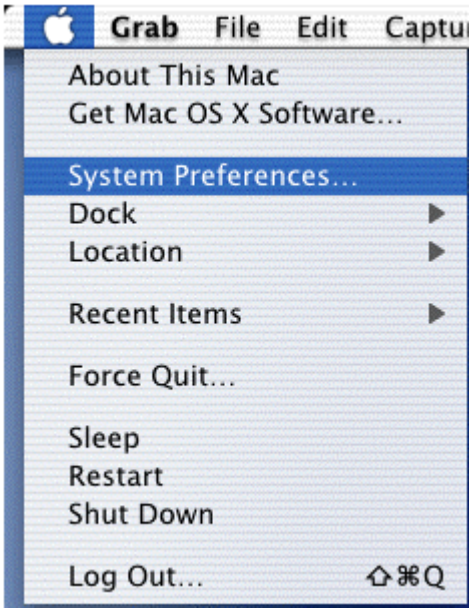
9. SETTING UP MACINTOSH OS X

This section provides instructions on how to use Macintosh Operating System 10 with VersaLink. Follow the instructions in this section to create a new network configuration for Macintosh OS X.

NOTE: Macintosh computers must use VersaLink's Ethernet installation. Refer to section 6, (INSTALLING THE HARDWARE).

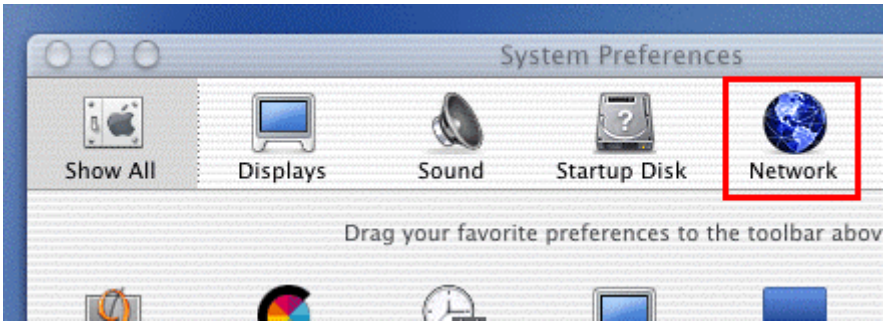
Opening the System Preference Screen

After you have connected the Westell VersaLink to the Ethernet port of your Macintosh, the screen below will appear. Click on the "**Apple**" icon in the upper-right corner of the screen and select **System Preferences**.



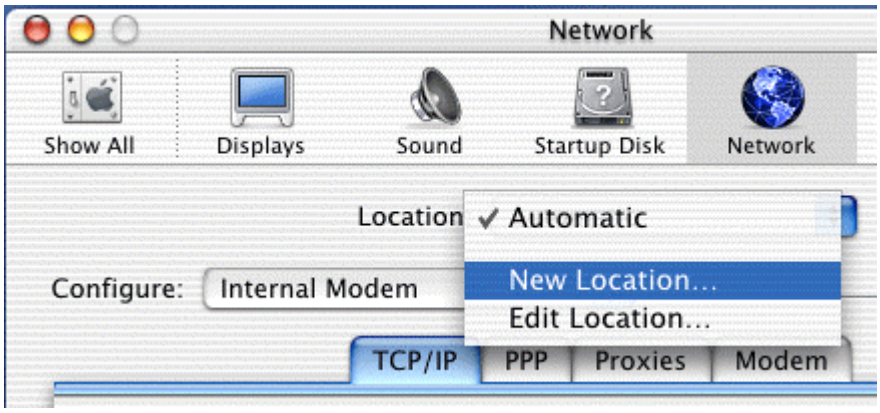
Choosing the Network Preferences

After selecting **System Preferences . . .**, from the previous screen, the **System Preferences** screen will be displayed. From the **System Preferences** screen, click on the **Network** icon.



Creating a New Location

After selecting the **Network** icon at the **System Preferences** screen, the **Network** screen will be displayed. Select **New Location . . .** from the **Location** field.



Naming the New Location

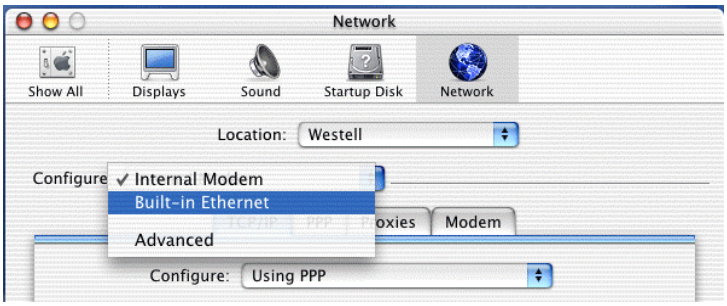
After selecting **New Location** from the **Network** screen, the following screen will be displayed. In the field labeled **Name your new location:**, change the text from "**Untitled**" to "**Westell**." Click **OK**.

Name your new location:
Westell
All users of this computer will be able to choose this location in the Apple menu without entering a password.
Cancel
OK

Selecting the Ethernet Configuration

After clicking on **OK** in the preceding screen, the **Network** screen will be displayed. The **Network** screen shows the settings for the newly created location. From the **Configure** field in the **Network** screen, select **Built-in Ethernet**. Click on **Save**.

NOTE: Default settings for the Built-in Ethernet configuration are sufficient to operate VersaLink.

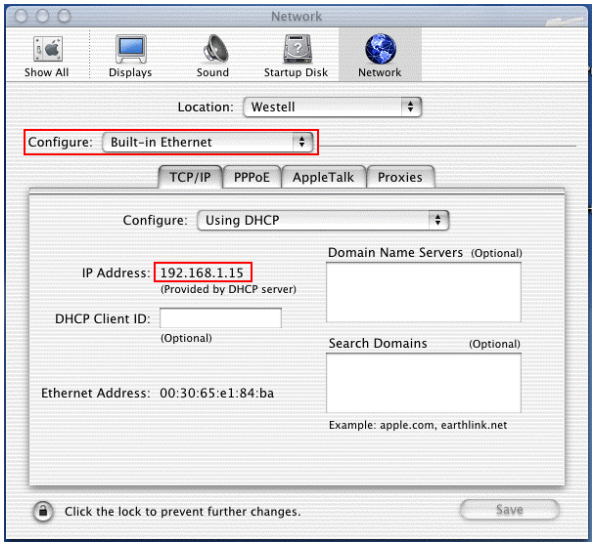


Checking the IP Connection

To verify that the computer is communicating with VersaLink, follow the instructions below.

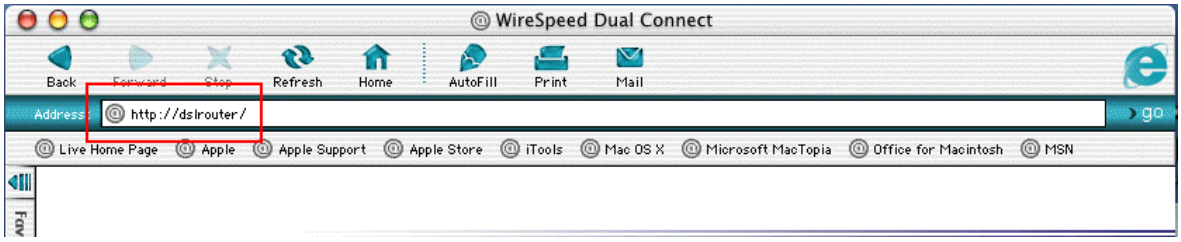
1. Go to the "**Apple**" icon in the upper-right corner of the screen and select **System Preferences**.
2. From the **System Preferences screen**, click on the **Network** icon. The **Network** screen will be displayed.
3. From the **Configure** field in the **Network** screen, select **Built-in Ethernet**.
4. View the IP address field. An IP address that begins with **192.168.1** should be displayed.

NOTE: The DHCP server provides this IP address. If this IP address is not displayed, check VersaLink's wiring connection to the PC. If necessary, refer to section 6 for hardware installation instructions.

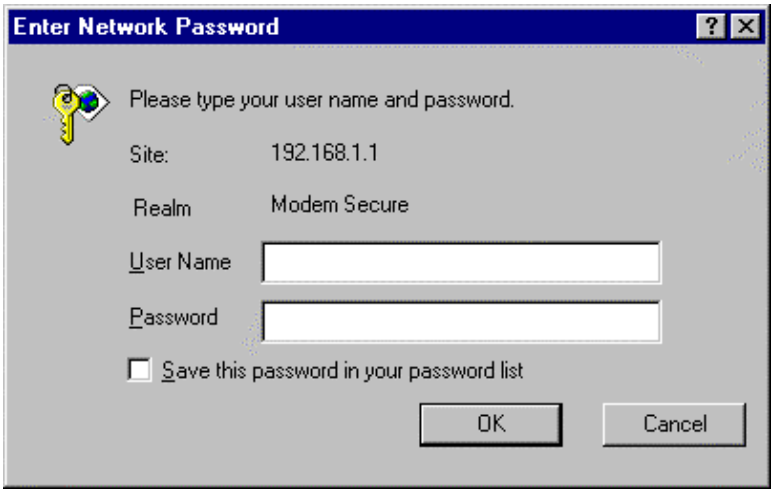


Accessing Your VersaLink

In the address window of your Internet Explorer web browser, type **http://dslrouter/**. Press 'Enter' on your keyboard.



The **Enter Network Password** screen will be displayed. You may now begin your network logon. Proceed to the **Enter Network Password** screen in section 7.1 of this User Guide for logon instructions.



The following sections explain the advanced features of VersaLink™.

[This Page Intentionally Left Blank]

10. SETTING UP ADVANCED CONFIGURATION

Advanced Configuration instructions are explained in Section 11 through Section 17. If you want to set up advanced features for VersaLink, follow the instructions provided in sections 11 through 17.

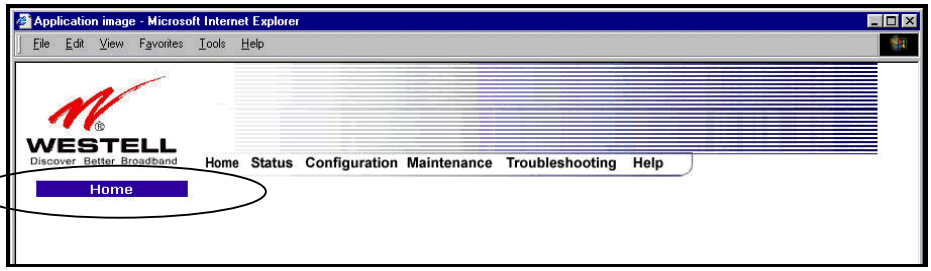
IMPORTANT: The following sections assume that you have active DSL and Internet service.

VersaLink allows you to make changes to advanced features of your Gateway such as account profiles, routing configurations, firewall settings. The following sections explain each feature and show you how to make changes to VersaLink's settings. The main menu, displayed at the top of each page, allows you to navigate you to the various configuration screens of your VersaLink Gateway. Whenever you change the configurable settings of your Gateway, you must click **save** to allow the changes to take effect. If you are at a screen and need help, click on **Help** to learn more about that screen.

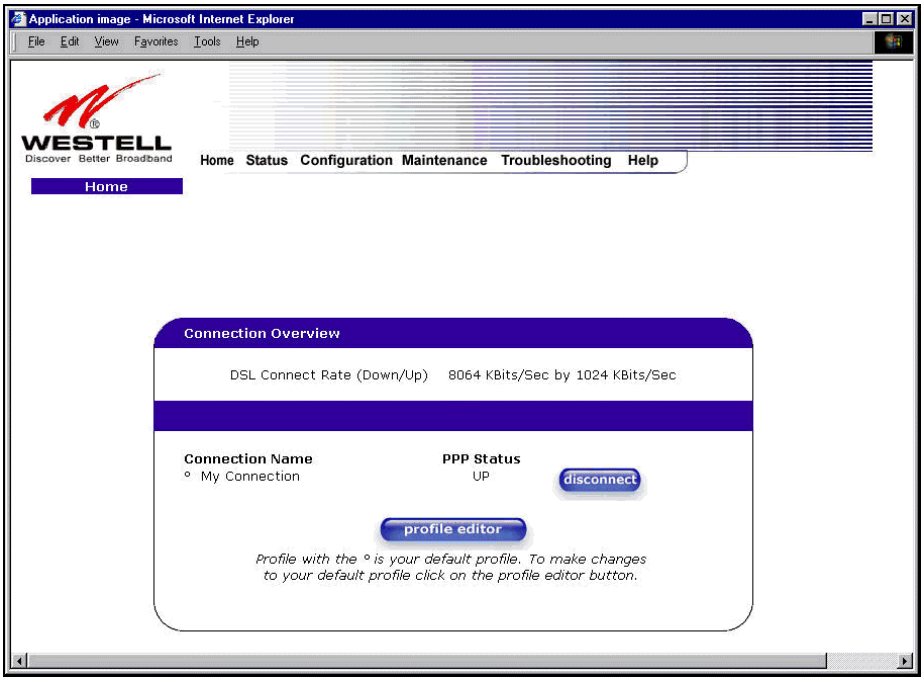
Please note that the menu options displayed will vary according to the WAN configuration you have chosen to use, DSLATM PORT or ETHERNET PORT1. However, all menu options are displayed when VersaLink is enabled for DSLATM PORT. Instructions on enabling and disabling DSLATM PORT and ETHERNET PORT 1 are explained in section 13.6, Advanced WAN. This document was created with VersaLink in DSLATM PORT mode. The sections explained throughout this document will indicate when a menu item is unavailable.

11. HOME

As you navigate through the various screens of VersaLink, the name of the active page that you have selected will appear in the upper-left corner of the screen, as shown below. Please note that the actual values reported by your Gateway may differ from the values displayed in the screens.



If you have set up your account profile and established your PPP session, as discussed in section 8.3, "Establishing a PPP Session," the following screen will be displayed if you click **Home** in the main menu.

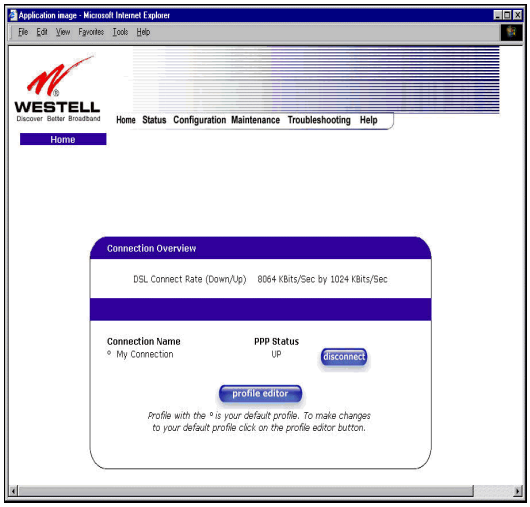

Application image - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Home
Connection Overview
DSL Connect Rate (Down/Up) 8064 KBits/Sec by 1024 KBits/Sec
Connection Name
° My Connection
PPP Status
UP
disconnect
profile editor
Profile with the ° is your default profile. To make changes to your default profile click on the profile editor button.

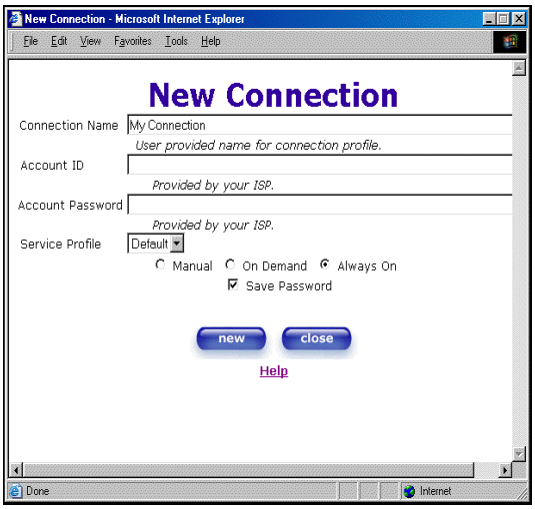
Connection Overview	Displays your DSL connection rate.
Connection Name	This Connection Name is from the connection profile that you established in Section 8.
PPP Status	UP = PPP session established DOWN = No PPP session established.
Connect/Disconnect	CONNECT = Establish a PPP session DISCONNECT = Disconnect a PPP session
Profile Editor	This allows you to make changes to the profile that you created in Section 8.

11.1 Adding Account Profiles

To add an account profile, click the **Profile Editor** button in **Home** screen; the **New Connection** screen will appear. Enter your profile information (the Account ID and Account password must be the same values that you entered in section 8.2) and then click **New**. Next, click **OK** in the **"Save new connection?"** pop-up screen to save your settings. If you do not want to save the new connection, click **cancel** in the pop-up screen.

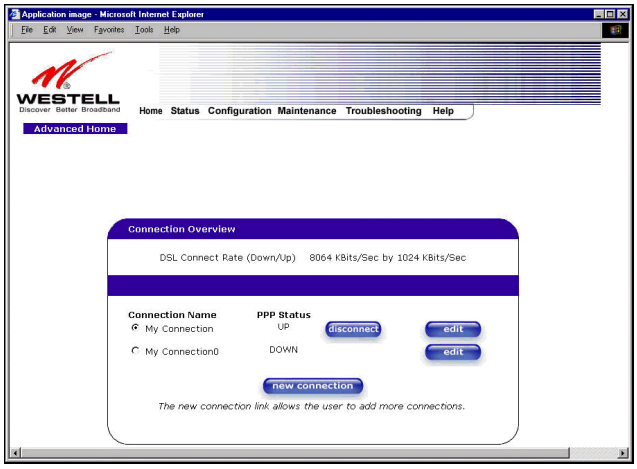
NOTE: NAT Profiles allow you to create specific service settings. A NAT Profile may be associated with a certain connection setting, or NAT services. This allows you to customize the profile for specific users. You may store up to eight unique user profiles in your VersaLink Gateway. Details on the **New Connection** screen are located at the end of this section.


Application image - Microsoft Internet Explorer
WESTELL
Home Status Configuration Maintenance Troubleshooting Help
Home
Connection Overview
DSL Connect Rate (Down/Up) 8064 KBits/Sec by 1024 KBits/Sec
Connection Name
° My Connection
PPP Status
UP
disconnect
profile editor
Profile with the ° is your default profile. To make changes to your default profile click on the profile editor button.



After you have clicked **OK** in the **"Save new connection?"** pop-up screen, the following screen will be displayed. This screen displays the new profile "My Connection0."

IMPORTANT: Although you have added new profile, your Internet connection will be available only for the default profile, which you have set up in section 8.2. To establish a PPP session and browse the Internet using the new profile, you must first configure the new profile as the default account profile. To do this, click the radio button adjacent to the connection name that want to use as your default connection profile. Next click **OK** when asked **"Do you wish to change the Default Connection Profile?"**

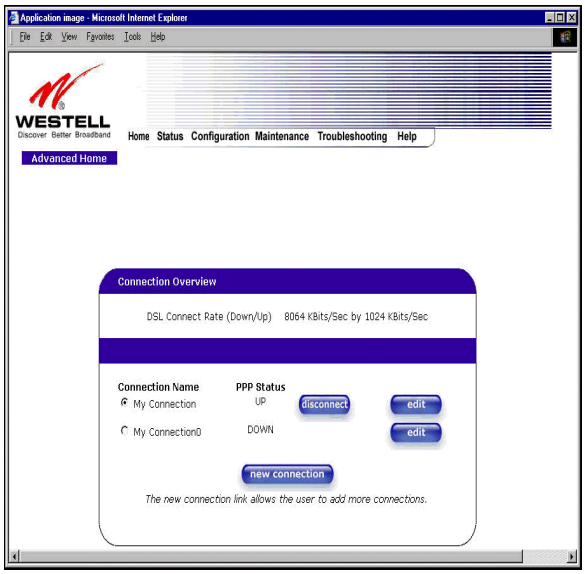


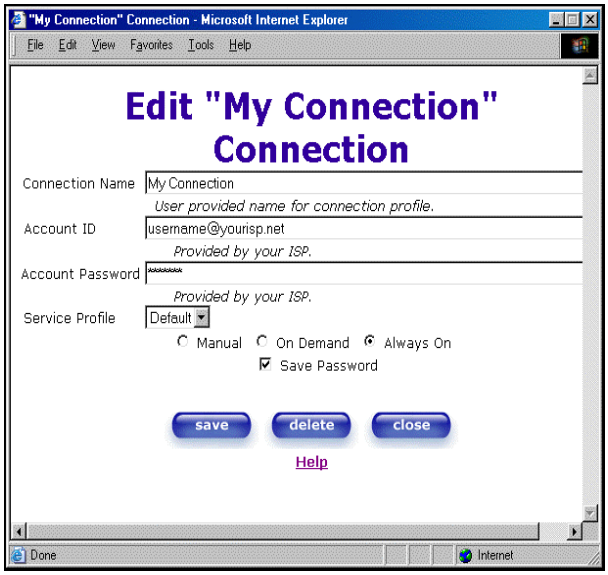
11.2 Editing Account Profiles

To edit an account profile, click the **edit** button adjacent to the connection name that you want to edit. The **Edit "My Connection"** screen will appear.

NOTE: If you have created multiple account profiles, first select the option button for the active account profile.

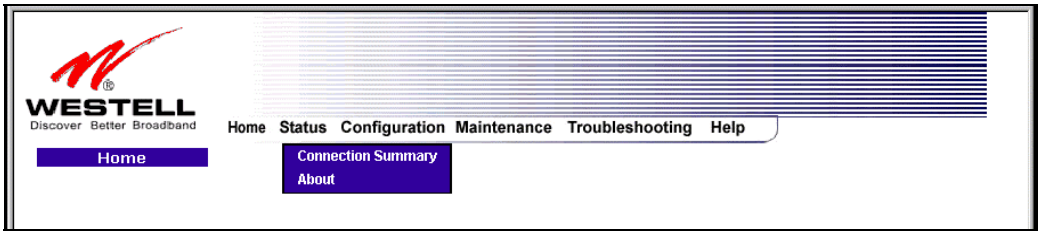
Next, enter the desired values in the **Edit "My Connection"** and click **save.** Click **OK** in the pop-up screen to save the changes. If you do not want to save the changes, click **cancel** in the pop-up screen. Click **delete** if you want to delete the profile.





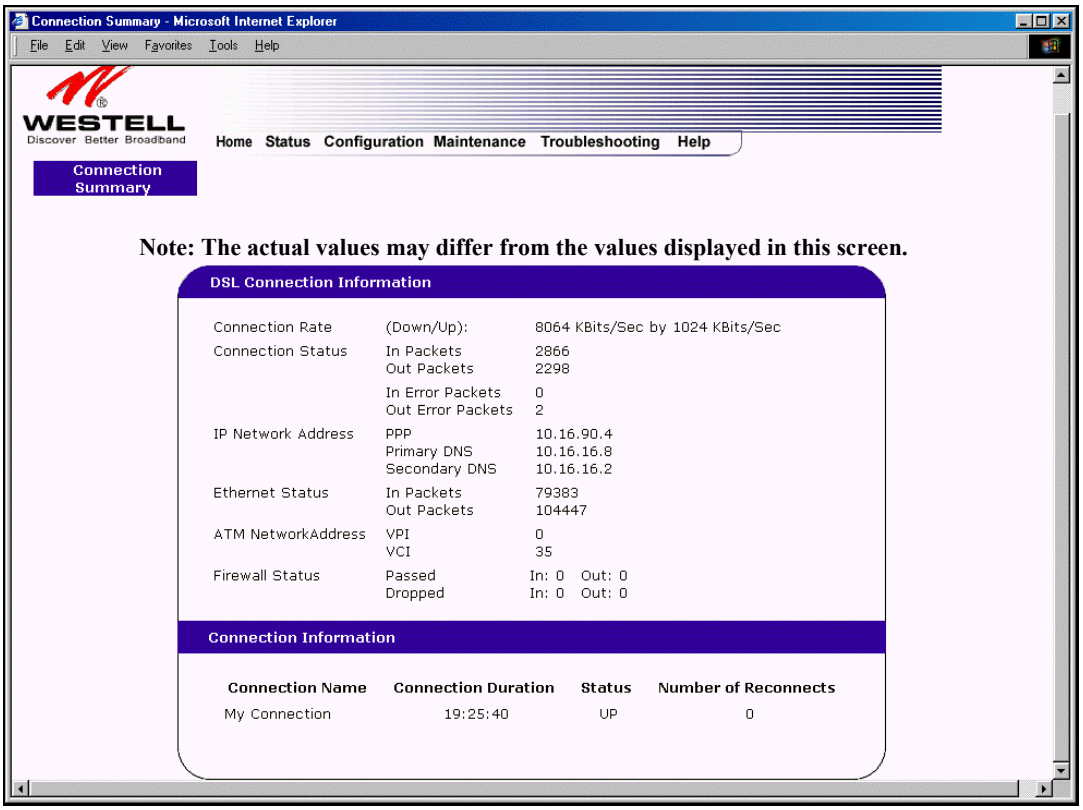
Edit My Connection	
Connection Name	This field allows you to enter a new connection name of your choice (up to 64 characters).
Account ID	The account ID that you used in section 8, provided by your ISP.
Account Password	The account password that you used in section 8, provided by your ISP.
Service Profile	Westell recommends that you use the Default parameter.
Manual	Selecting this feature allows you to manually establish your PPP session.
On Demand	Selecting this feature allows the Gateway to automatically re-establish your PPP session on demand anytime your PC requests Internet activity (for example, browsing the Internet, email, etc.). When you have traffic, it may cause a delay.
Always On (Factory Default)	Selecting this feature allows the Gateway to automatically establish a PPP session when you log on, or if the PPP session goes down.
Save Password	Selecting this feature allows you to save the password for your new connection profile in VersaLink so that you will not have to reenter it in case of a reboot.

12. STATUS



12.1 Connection Summary

The following screen will be displayed if you select **Connection Summary** from the **Status** menu.

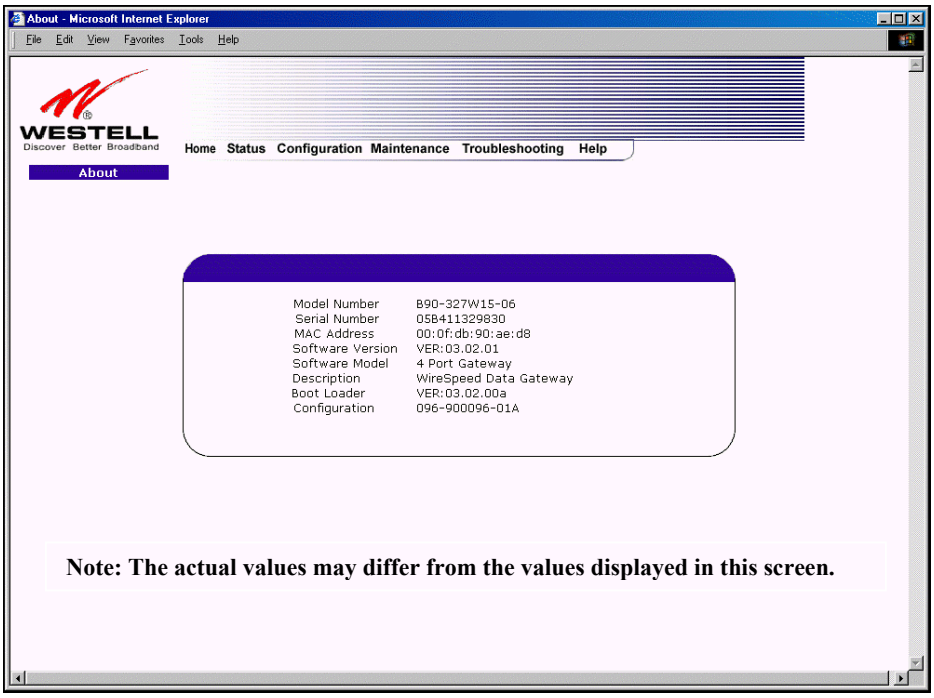

Connection Summary - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Connection Summary
Note: The actual values may differ from the values displayed in this screen.
DSL Connection Information
Connection Rate (Down/Up): 8064 KBits/Sec by 1024 KBits/Sec
Connection Status In Packets 2866
Out Packets 2298
In Error Packets 0
Out Error Packets 2
IP Network Address PPP 10.16.90.4
Primary DNS 10.16.16.8
Secondary DNS 10.16.16.2
Ethernet Status In Packets 79383
Out Packets 104447
ATM NetworkAddress VPI 0
VCI 35
Firewall Status Passed In: 0 Out: 0
Dropped In: 0 Out: 0
Connection Information
Connection Name Connection Duration Status Number of Reconnects
My Connection 19:25:40 UP 0

DSL Connection Information	
Connection Rate	This field will let you know if you have a DSL signal and the DSL rate at which you are connected.
Connection Status	This field will show how much information was received (IN) or sent (OUT) in packets.
IP Network Address	PPP = An IP address identifies your device on the Internet Primary DNS = Provided by your ISP Secondary DNS = Provided by ISP
Ethernet Status	This field will display your Ethernet information that was received (IN) or sent (OUT) in

	packets on your Ethernet port.
ATM Network Address	This field will display your VPI and VCI values, which are provided by your ISP.
Firewall Status	This field will display your firewall traffic in packets. Passed: Monitors information traffic that was successfully received (IN) or transmitted (OUT) in packets. Dropped: Monitors information traffic that was not successfully received (IN) or transmitted (OUT) due to your firewall settings.
PPP Connection Information	
Connection Name	This is from the connection profile that you established in section 8.
Connection Duration	This field will display how long your PPP session has been connected.
Status	This field will display the status of your PPP session. UP=Connected DOWN=Disconnected
Number of Reconnects	This field will display the number of attempts that were made to establish a PPP session.

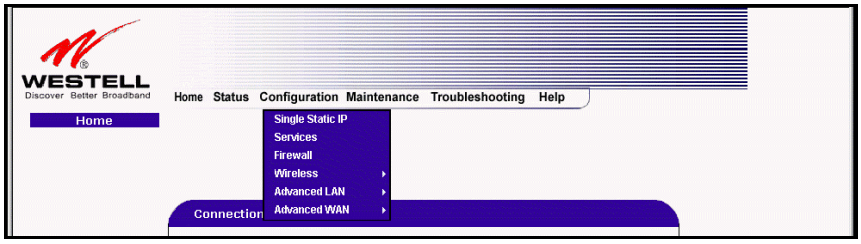
12.2 About

The following screen will be displayed if you select **About** from the **Status** menu.


About - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
About
Model Number B90-327W15-06
Serial Number 05B411329830
MAC Address 00:0f:db:90:ae:d8
Software Version VER:03.02.01
Software Model 4 Port Gateway
Description WireSpeed Data Gateway
Boot Loader VER:03.02.00a
Configuration 096-900096-01A
Note: The actual values may differ from the values displayed in this screen.

Model Number	VersaLink manufacturer's model number.
Serial Number	VersaLink manufacturer's serial number.
MAC Address	Media Access Controller (MAC) i.e., hardware address of this device.
Software Version	Version of Application Software.
Software Model	VersaLink application type.
Description	Product description.
Boot Loader	Version of boot loader software
Configuration	Proprietary configuration number of this device.

13. CONFIGURATION



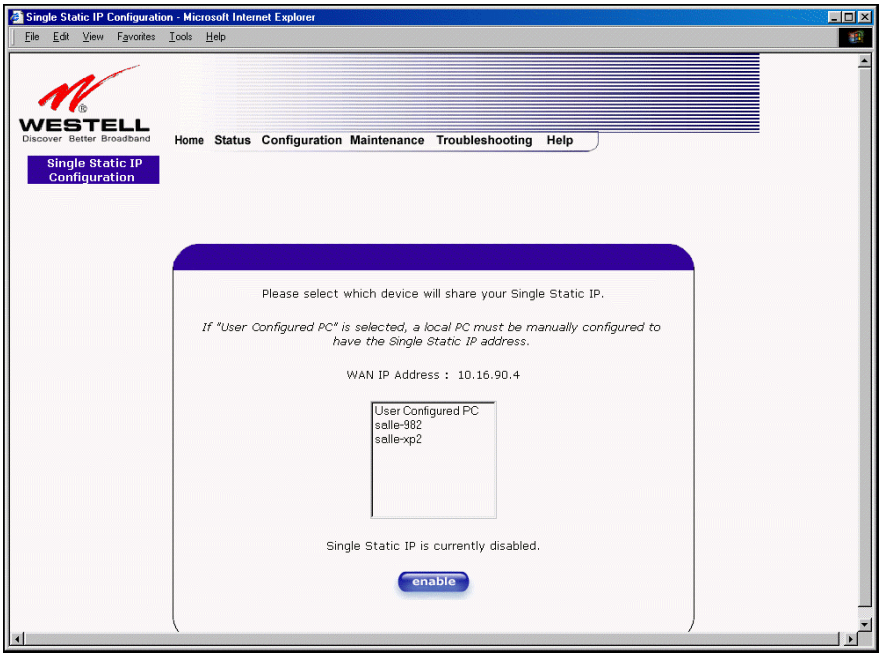
13.1 Single Static IP – Single IP Address PassThrough

IMPORTANT:
1) Before you begin this section, configure your PC settings to obtain an IP address from VersaLink automatically. If needed, refer to your computer's Windows® help screen for instructions.

2) Static NAT and Single Static IP are mutually exclusive features. Static NAT should be disabled (if it has previously been enabled) before you enable **Single Static IP**. To disable Static NAT, select **Services** from the **Configuration** menu. Next, click the **static NAT** button. Select the device from the **Static NAT Device** drop-down menu and click **disable**. You may now configure Single Static IP.

The following screen will be displayed if you select **Single Static IP** from the **Configuration** menu.

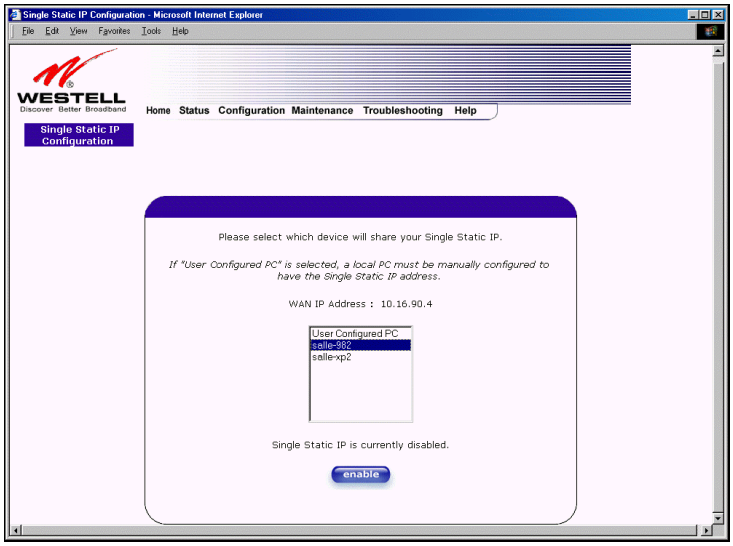
Single Static IP (SSI) allows the user to select one device on your LAN that will share the WAN assigned IP address. By doing this, the device with the SSI becomes visible on the Internet. Network Address Translation (NAT) and Firewall rules do not apply to the device configured for SSI. If you are using Bridge (Routed Bridge) protocol, **Single Static IP** configuration will not be available.


Single Static IP Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Single Static IP Configuration
Please select which device will share your Single Static IP.
If "User Configured PC" is selected, a local PC must be manually configured to have the Single Static IP address.
WAN IP Address : 10.16.90.4
User Configured PC
salle-982
salle-xp2
Single Static IP is currently disabled.
enable

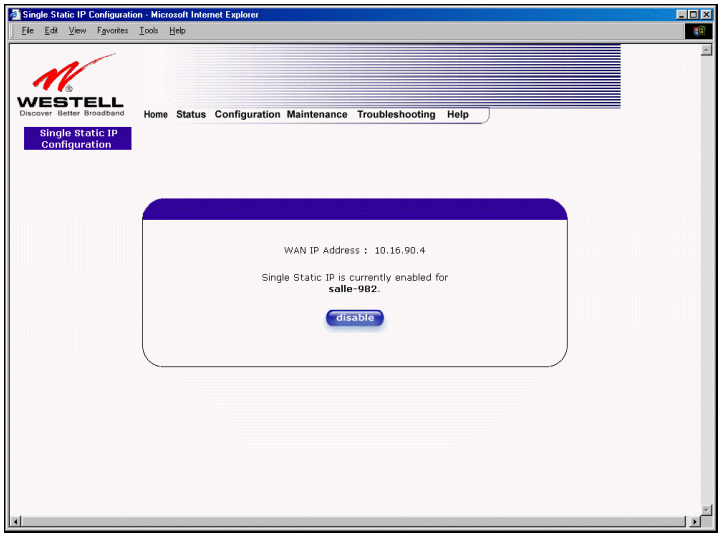
13.1.1 Enabling Single Static IP – Single IP Address PassThrough (Applicable for PPPoA/PPPoE Connections Only)

To enable Single Static IP, select a device that will share your Single Static IP from the options listed in the window. Click **enable** to enable Single Static IP for the selected device.

NOTE: The Single Static IP Configuration screen allows you to select the device on your LAN that will share your Single Static IP.


Single Static IP Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Single Static IP Configuration
Please select which device will share your Single Static IP.
If "User Configured PC" is selected, a local PC must be manually configured to have the Single Static IP address.
WAN IP Address : 10.16.90.4
User Configured PC
salle-982
salle-xp2
Single Static IP is currently disabled.
enable

Next, Select **Single Static IP** from the **Configuration** menu to confirm that Single Static IP has been **enabled**, as shown in the following screen.

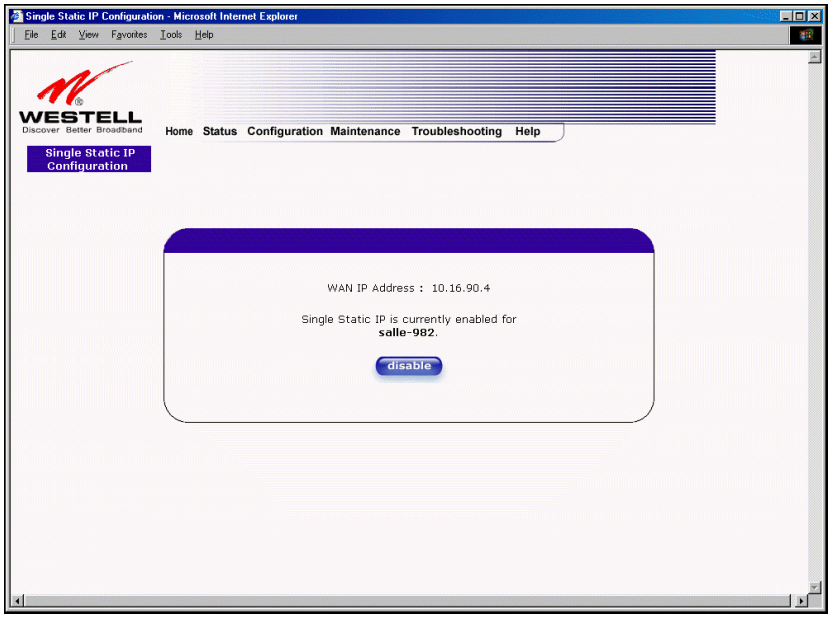

Single Static IP Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Single Static IP Configuration
WAN IP Address : 10.16.90.4
Single Static IP is currently enabled for
salle-982.
disable

IMPORTANT: After you enable Single Static IP, reboot your computer to allow the changes to take effect.

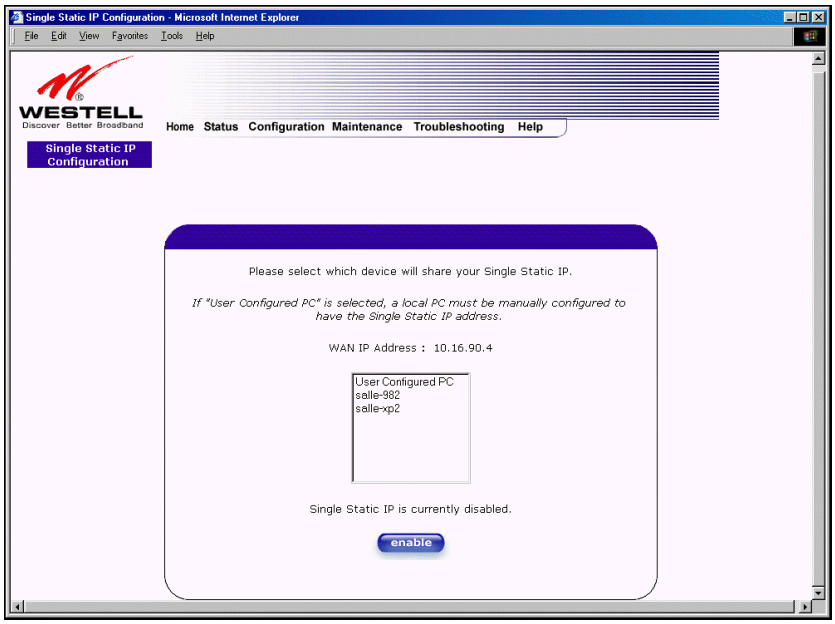
NOTE: If you chose to enable **User Configured PC,** wait for the Gateway to reset, and then manually enter the WAN IP, Gateway, and Subnet mask addresses you obtained from your ISP into a PC.

13.1.2 Disabling Single Static IP – Single IP Address PassThrough

To disable Single Static IP, select **Single Static IP** from the **Configuration** menu. Click **disable** to disable single static IP for the selected device.


Single Static IP Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Single Static IP Configuration
WAN IP Address : 10.16.90.4
Single Static IP is currently enabled for salle-982.
disable

Next, select **Single Static IP** from the **Configuration** menu to confirm that Single Static IP is **disabled**, as shown in the following screen.


Single Static IP Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Single Static IP Configuration
Please select which device will share your Single Static IP.
If "User Configured PC" is selected, a local PC must be manually configured to have the Single Static IP address.
WAN IP Address : 10.16.90.4
User Configured PC
salle-982
salle-xp2
Single Static IP is currently disabled.
enable

IMPORTANT: After you disable Single Static IP, reboot your computer to allow the changes to take effect.

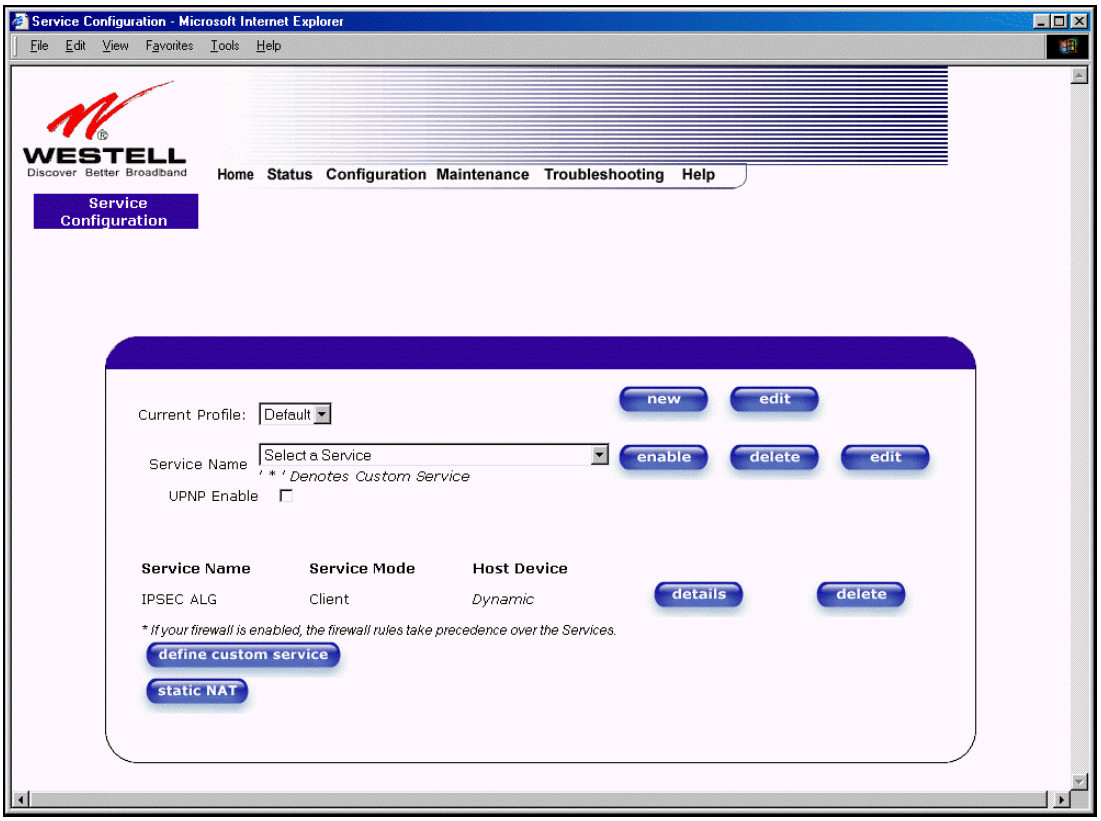
13.2 Service Configuration

The following screen will be displayed if you select **Services** from the **Configuration** menu.

Westell has developed an extensive list of NAT services and you may select any service from this list. By selecting your specific NAT service and setting up a NAT profile, you will ensure that the appropriate ports on VersaLink are open and that the required application traffic can pass through your LAN. For a list of supported services, go to section 17 (NAT Services).

NAT Profiles allow you to create specific service settings. The NAT profile may then be associated with a connection profile, allowing you to customize profiles for specific users. For example, if you want to attach specific NAT services to a profile, or if you want to set up a different connection setting for a profile, you can create new NAT profiles and customize them to your preference.

NOTE: You may create up to four NAT profiles and attach an unlimited number of services to each profile.


Service Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Service Configuration
Current Profile: Default
new edit
Service Name Select a Service
enable delete edit
' * ' Denotes Custom Service
UPNP Enable
Service Name Service Mode Host Device
IPSEC ALG Client Dynamic
details delete
* If your firewall is enabled, the firewall rules take precedence over the Services.
define custom service
static NAT

Current Profile	Displays the NAT (Network Address Translation) services that you have selected.
Service Name	Drop down selection menu of NAT (Network Address Translation) service you can select to configure you VersaLink.
UPNP Enable	Factory Default = Disable Enabling UPNP (Universal Plug and Play) allows automatic device discovery by your operating system.

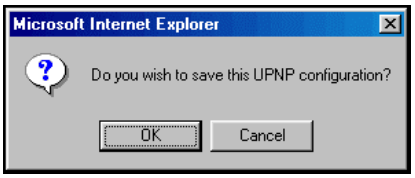
13.2.1 Configuring UPNP on the VersaLink

To enable UPNP on your VersaLink Gateway perform the following steps:

1) Select **Service Configuration** from the Configuration screen
2) Click the **UPNP Enable** box (a check mark will appear in the box).
3) Follow the instructions in the pop-up screens.
4) Click **OK** to Reset the Gateway.

NOTE: When you are ready to disable UPNP, uncheck the **UPNP Enable** box in the **Service Configuration** screen.

If you click the **UPNP Enable** box in the **Service Configuration** screen, a check mark will appear in the box and the following pop-up screen will be displayed. Click **OK.**

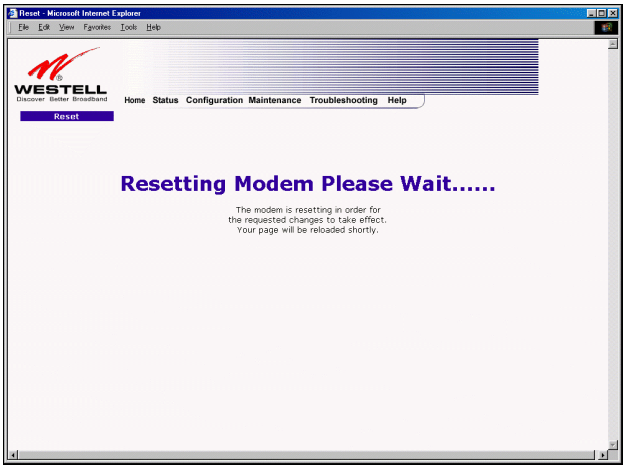


If you clicked **OK** in the preceding screen, the following pop-up screen will be displayed. Click on **OK** to continue.

Microsoft Internet Explorer
The modem must be reset in order for the new configuration to take affect.
Do you wish to reset now?
OK
Cancel

Note: To use the UPNP functionality in Versalink, your Windows XP operating system must also support UPNP. Please contact your computer manufacturer to verify that UPNP is enabled in your Windows XP operating system.

If you clicked **OK** in the preceding screen**,** the following screen will be displayed. The Gateway will be reset automatically, and the new configuration will take effect.


Reset - Microsoft Internet Explorer
WESTELL
Home Status Configuration Maintenance Troubleshooting Help
Reset
Resetting Modem Please Wait.....
The modem is resetting in order for the requested changes to take effect.
Your page will be reloaded shortly.

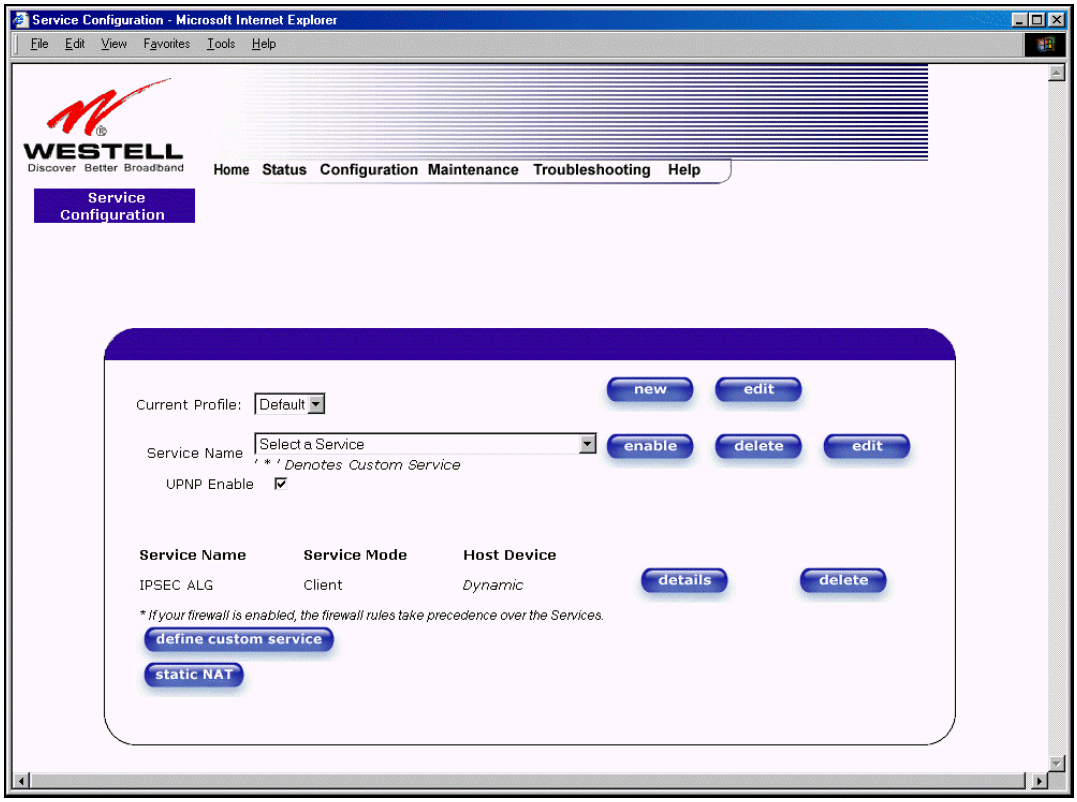
After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP.** (If necessary, click the **connect** button to establish a PPP session).

13.2.2 Creating a New Service Profile

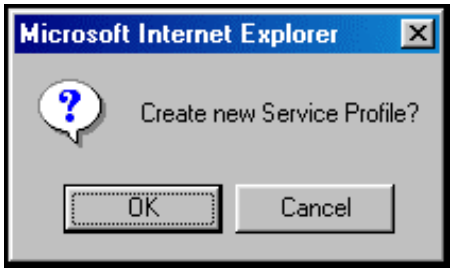
Service profiles allow you to create specific service settings. The service profile may then be associated with specific connection settings, allowing you to customize profiles for specific users. For example, if you want to attach specific NAT services to a profile, or if you want to set up a different connection setting for a profile, you can create new service profiles and customize them to your preference.

NOTE: You may create up to four service profiles and attach an unlimited number of services to each profile.

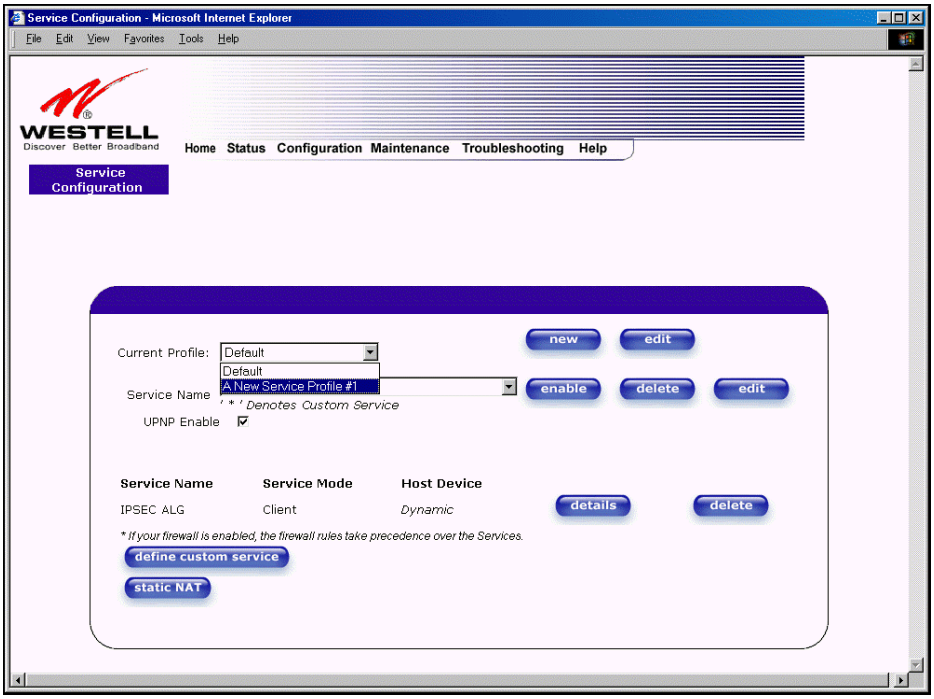
To create a new service profile, click **new** in the **Service Configuration** screen.



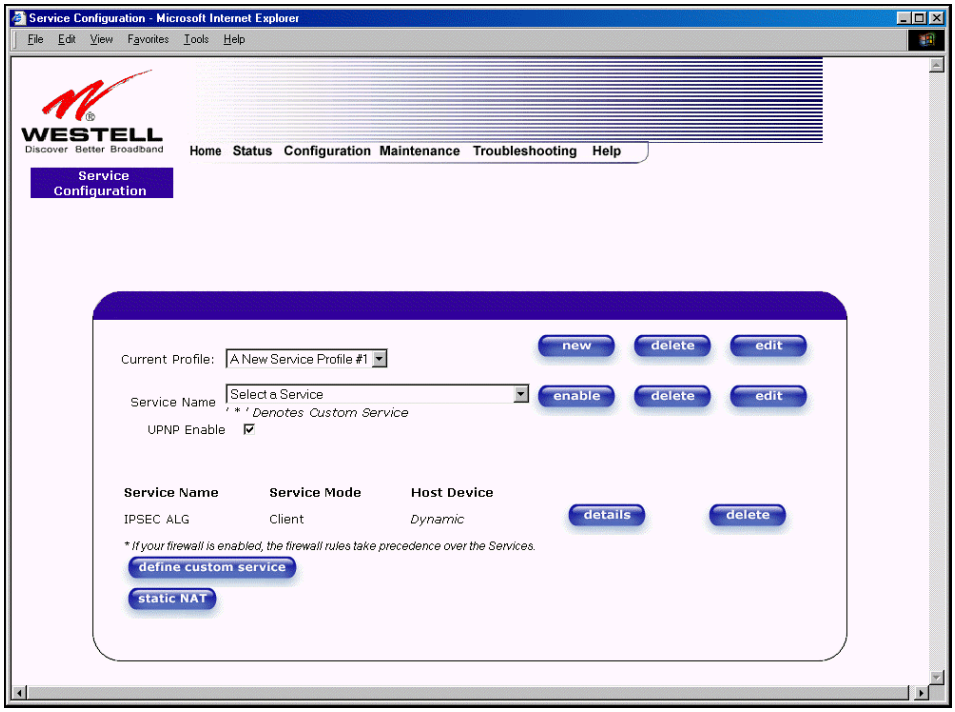
If you clicked **new** in the preceding **Service Configuration** screen, the **Create new Service Profile?** pop-up screen will be displayed. Click **OK** to begin creating your new service profile. Click **Cancel** if you do not want to create a new service profile.



If you clicked **OK**, the following screen will be displayed. Select **"A New Service Profile #1"** from the **Current Profile** drop-down arrow.


Service Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Service Configuration
Current Profile: Default
Default
A New Service Profile #1
new edit
Service Name
enable delete edit
' * ' Denotes Custom Service
UPNP Enable
Service Name Service Mode Host Device
IPSEC ALG Client Dynamic
details delete
* If your firewall is enabled, the firewall rules take precedence over the Services.
define custom service
static NAT

If you selected "**A New Service Profile #1,"** the following screen will be displayed. This screen shows that you have chosen to create a new service profile. You may create up to four service profiles and attach an unlimited number of NAT services to each profile.


Service Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Service Configuration
Current Profile: A New Service Profile #1
new delete edit
Service Name Select a Service
enable delete edit
' * ' Denotes Custom Service
UPNP Enable
Service Name Service Mode Host Device
IPSEC ALG Client Dynamic
details delete
* If your firewall is enabled, the firewall rules take precedence over the Services.
define custom service
static NAT

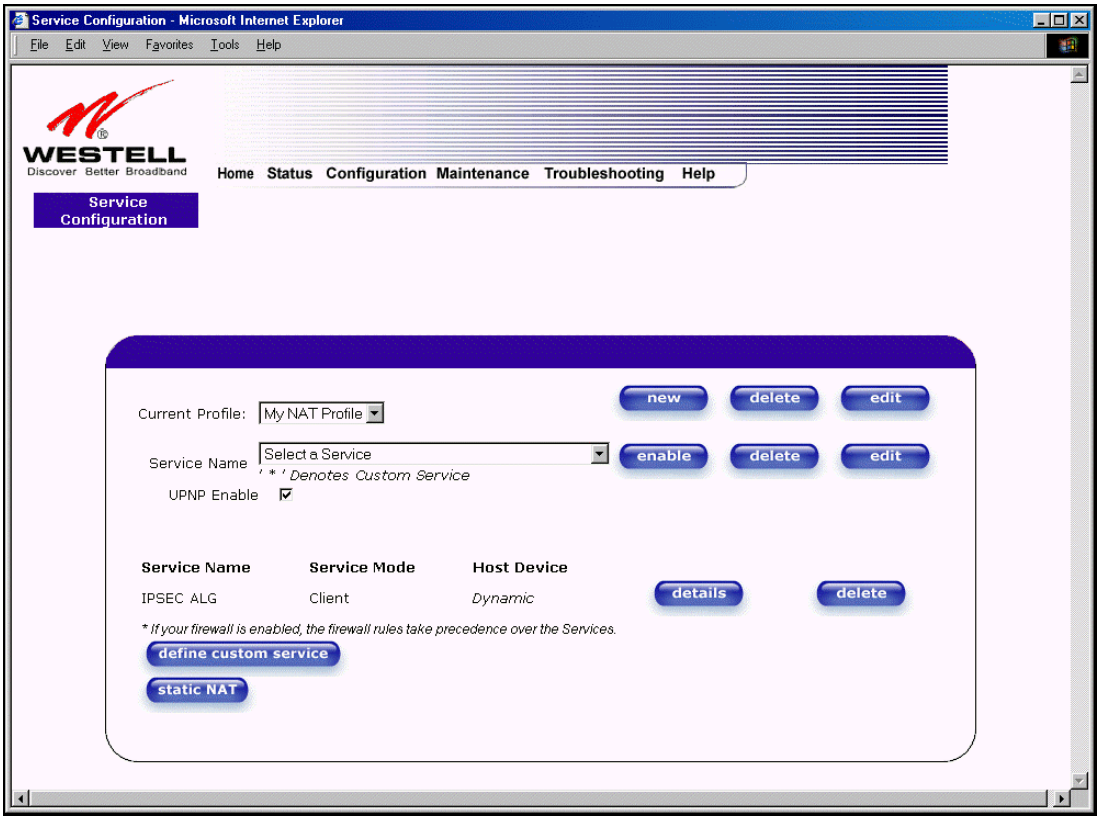
13.2.3 Editing a Service Profile Name

After you have created a service profile, you may edit the profile's name. To edit a profile name, select the **edit** button adjacent to **Current Profile** in the **Service Configuration** screen, the following screen will be displayed. Type your new profile name in the field labeled **Profile Name**.

The following screen shows that the profile name, "**My NAT Profile,**" was entered into the **Profile Name** field. Next, click **save** to save the new profile name. If you do not want to save the new profile name, click **close**.

If you clicked **save** in the **Edit Service Profile** screen, the following pop-up screen will be displayed. Click **OK** to save your new profile name.

The following screen displays the current profile. You may now add NAT services to your profile. Or, if desired, delete or edit an existing profile.


Service Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Service Configuration
Current Profile: My NAT Profile
new delete edit
Service Name Select a Service
' * ' Denotes Custom Service
enable delete edit
UPNP Enable
Service Name Service Mode Host Device
IPSEC ALG Client Dynamic
details delete
* If your firewall is enabled, the firewall rules take precedence over the Services.
define custom service
static NAT

13.2.4 Adding NAT Services to a Profile

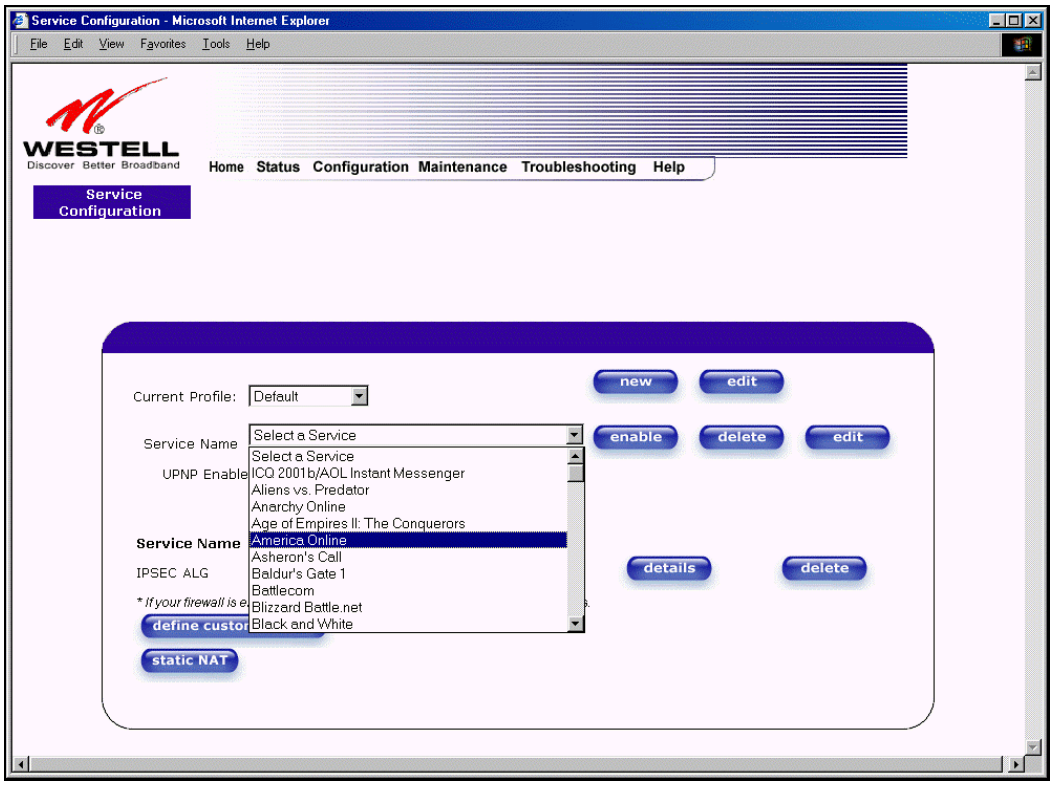
This section explains how to add NAT services to your profile. Remember, you may attach an unlimited number of NAT services to any profile.

NOTE: Westell has developed an extensive list of NAT services and you may select any service from this list. By selecting your specific NAT service and setting up a NAT profile, you will ensure that the appropriate ports on VersaLink are open and that the required application traffic can pass through your LAN. For a list of supported NAT services, see section 17 (NAT Services).

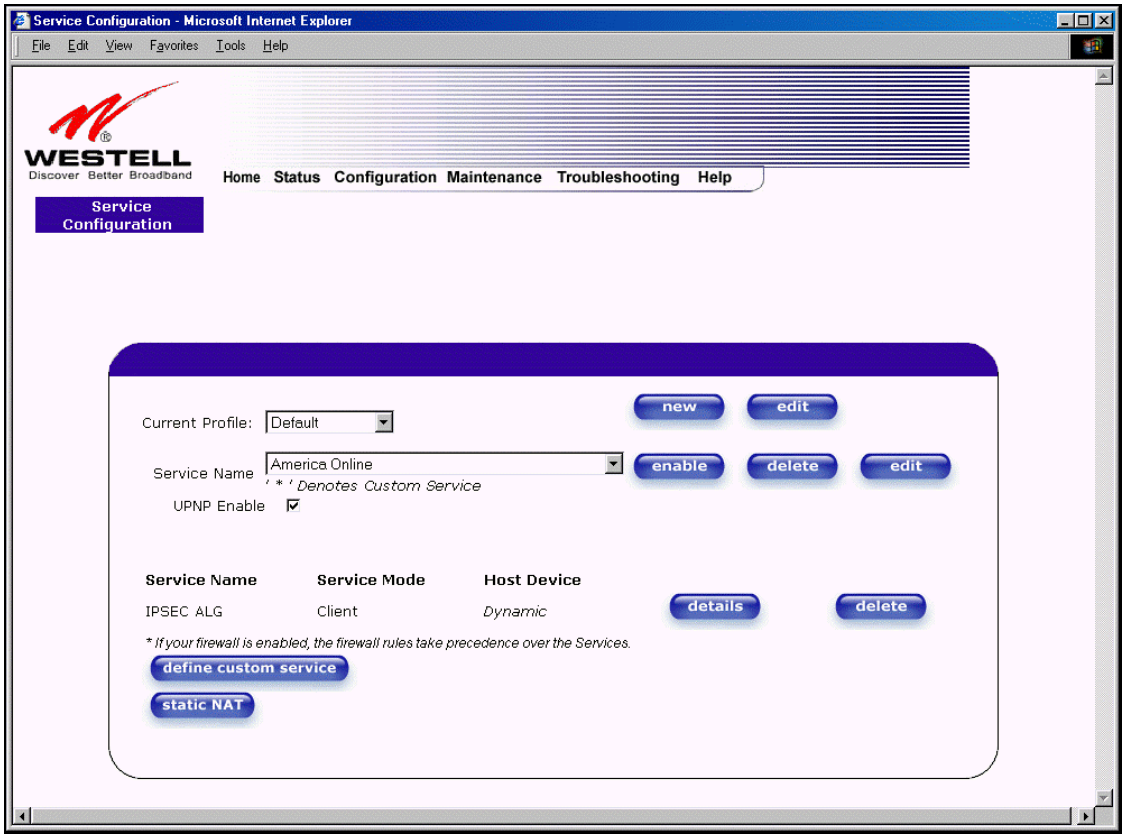
To add a NAT service, select **Services** from the **Configuration** menu. Next, select a NAT service from the options provided at the **Service Name** drop-down arrow.

NOTE: You can attach multiple NAT services to your profile. However, for each NAT service that you attach to your profile, you will need to first select the service profile from the **Current Profile** drop-down menu, and then add the new NAT service, as explained in this section.

In the following screen, the 'Default' profile has been selected as the profile that will host the selected NAT service, "America Online"; however, you may add NAT services to any profile name.

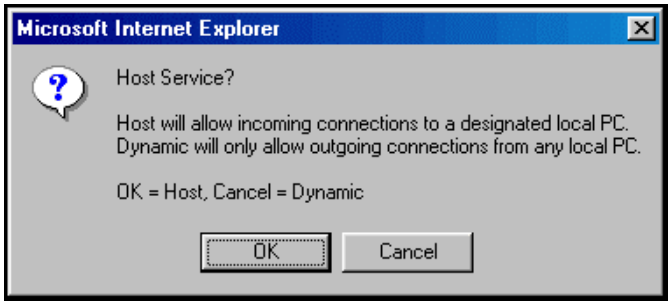


For example, the screen below displays **America Online** as the NAT service that has been selected. After you have selected a service, click **enable.**

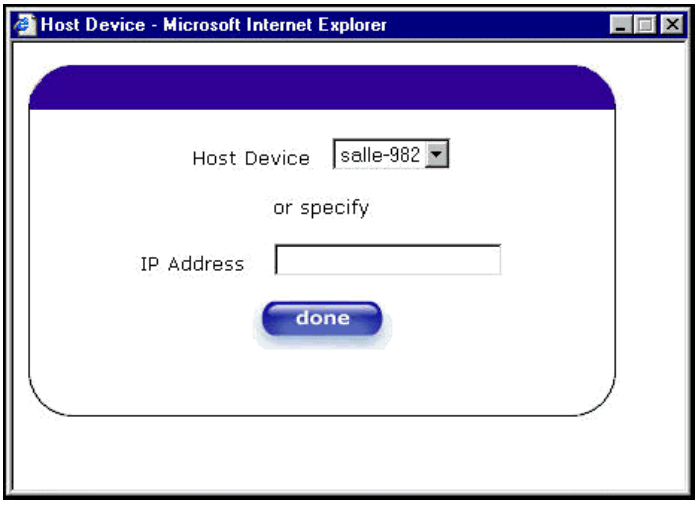

Service Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Service Configuration
Current Profile: Default
new edit
Service Name America Online
enable delete edit
' * ' Denotes Custom Service
UPNP Enable
Service Name Service Mode Host Device
IPSEC ALG Client Dynamic
details delete
* If your firewall is enabled, the firewall rules take precedence over the Services.
define custom service
static NAT

If you click **enable**, the following pop-up screen will be displayed. If you click **OK**, you will allow incoming connections to be forwarded to a designated local PC. If you click **Cancel**, you will allow only outgoing connections from any local PC. Click **OK** or click **Cancel.**

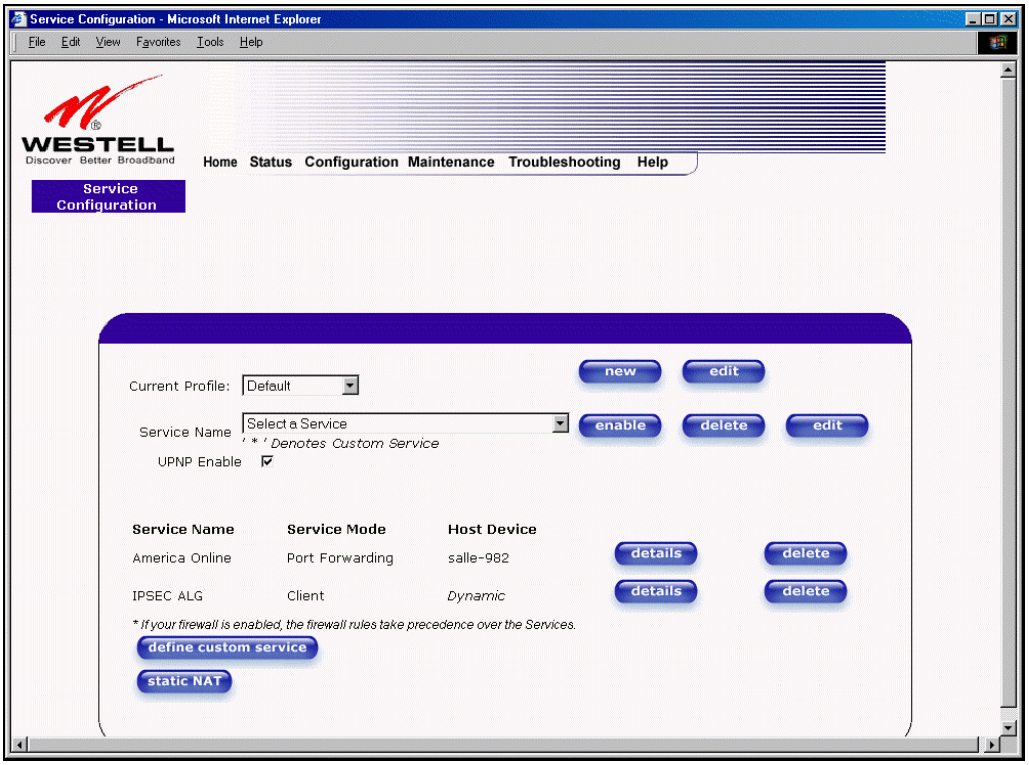
NOTE: If you click **Cancel** in the following pop-up screen, the NAT service you selected in the **Service Configuration** screen is still configured; however, it will not be assigned to any device on the local LAN. You must click **OK** to host the NAT service.


Microsoft Internet Explorer
Host Service?
Host will allow incoming connections to a designated local PC.
Dynamic will only allow outgoing connections from any local PC.
OK = Host, Cancel = Dynamic
OK
Cancel

If you clicked **OK** in the preceding pop-up screen, the **Host Device** screen will be displayed. The **Host Device** screen allows you to select which device will host the NAT service you selected on your local area network. You must either select the device from the **Host Device** drop-down arrow or type an IP address in the field labeled **IP Address,** and then click **done** to continue.



After you have selected a NAT service and have saved it to your service profile, the following screen will be displayed. It displays the NAT service that has been added to the profile.


Service Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Service Configuration
Current Profile: Default
new edit
Service Name Select a Service
enable delete edit
' * ' Denotes Custom Service
UPNP Enable
Service Name Service Mode Host Device
America Online Port Forwarding salle-982
details delete
IPSEC ALG Client Dynamic
details delete
* If your firewall is enabled, the firewall rules take precedence over the Services.
define custom service
static NAT

If you click the **details** button adjacent to a NAT service in the **Service Configuration** screen, the following screen will display the details of the NAT service. If you click the **delete** button in the **Service Configuration** screen, you will remove that NAT service from your profile. Click **close** to continue.

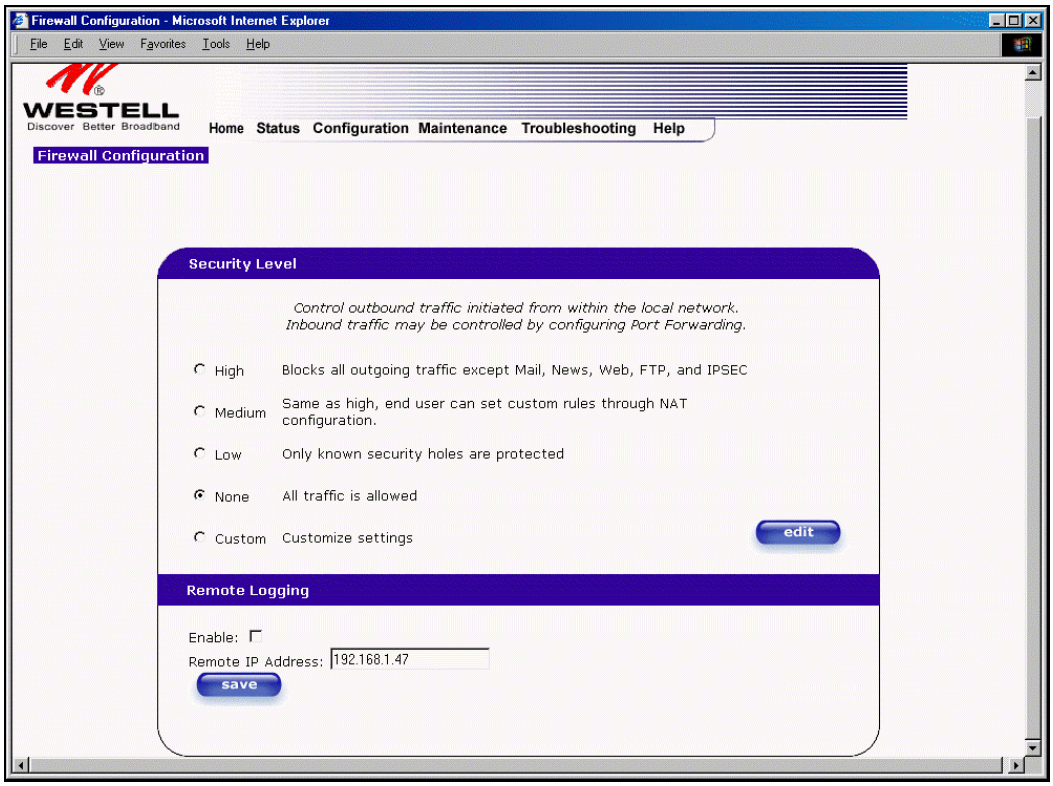
NOTE: If you want to set up additional Advanced Service Configuration options, refer to section 14, “Setting Up Advanced Service Configuration.”

13.3 Firewall Configuration

The following screen will be displayed if you select **Firewall** from the **Configuration** menu.

IMPORTANT: Westell recommends that you do not change the settings in the **User Defined Firewall Rules** screen. If you need to reset VersaLink to factory default settings, push the reset button on the rear of VersaLink.

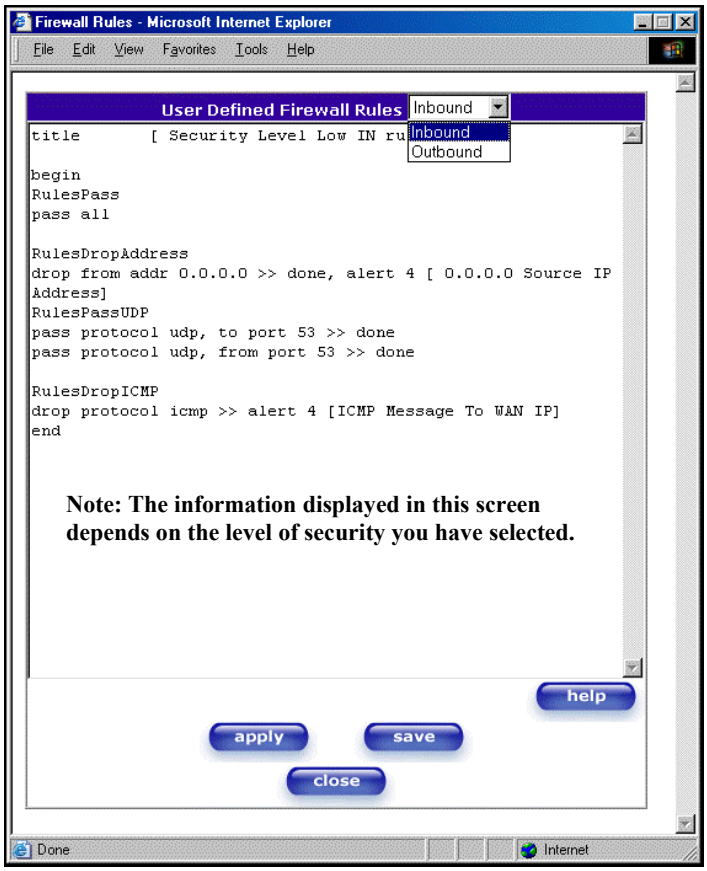
To change your firewall security level, select an option in the **Security Level** section, and then click **edit** to go to the **User Defined Firewall Rules** screen. If you select "None," no rules will be displayed in the **User Defined Firewall Rules** screen. (The factory default setting for the security level for VersaLink is **None.**)


Firewall Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Firewall Configuration
Security Level
Control outbound traffic initiated from within the local network.
Inbound traffic may be controlled by configuring Port Forwarding.
High Blocks all outgoing traffic except Mail, News, Web, FTP, and IPSEC
Medium Same as high, end user can set custom rules through NAT configuration.
Low Only known security holes are protected
None All traffic is allowed
Custom Customize settings
edit
Remote Logging
Enable:
Remote IP Address: 192.168.1.47
save

Security Level	
High	High security level only allows basic Internet functionality. Only Mail, News, Web, FTP, and IPSEC are allowed. All other traffic is prohibited.
Medium	Like High security, Medium security only allows basic Internet functionality by default. However, Medium security allows customization through NAT configuration so that you can enable the traffic that you want to pass.
Low	The Low security setting will allow all traffic except for known attacks. With Low security, VersaLink is visible to other computers on the Internet.
None (Factory Default)	Firewall is disabled. (All traffic is passed)
Custom	Custom is an advanced configuration option that allows you to edit the firewall configuration directly. NOTE: only the most advanced users should try this.
Remote Logging	
Enable	Factory Default = Disable If enabled, VersaLink will send firewall logs to a syslog server.
Remote IP Address	The IP address of the syslog server machine to which the diagnostics logs to be sent.

If you selected **Edit** in the **Firewall Configuration** screen, the following **User Defined Firewall Rules** screen will be displayed. The information displayed in this screen depends on the Firewall security setting you have selected. This screen allows you to change the security parameters on your Inbound and Outbound Firewall rules via the **User Defined Firewall Rules** drop-down arrow. If you select **Inbound**, this will restrict inbound traffic from the WAN to the LAN. **Outbound** restricts outbound traffic to the LAN from the WAN. To apply the new settings, click **Apply** in the screen labeled **User Defined Firewall Rules**.

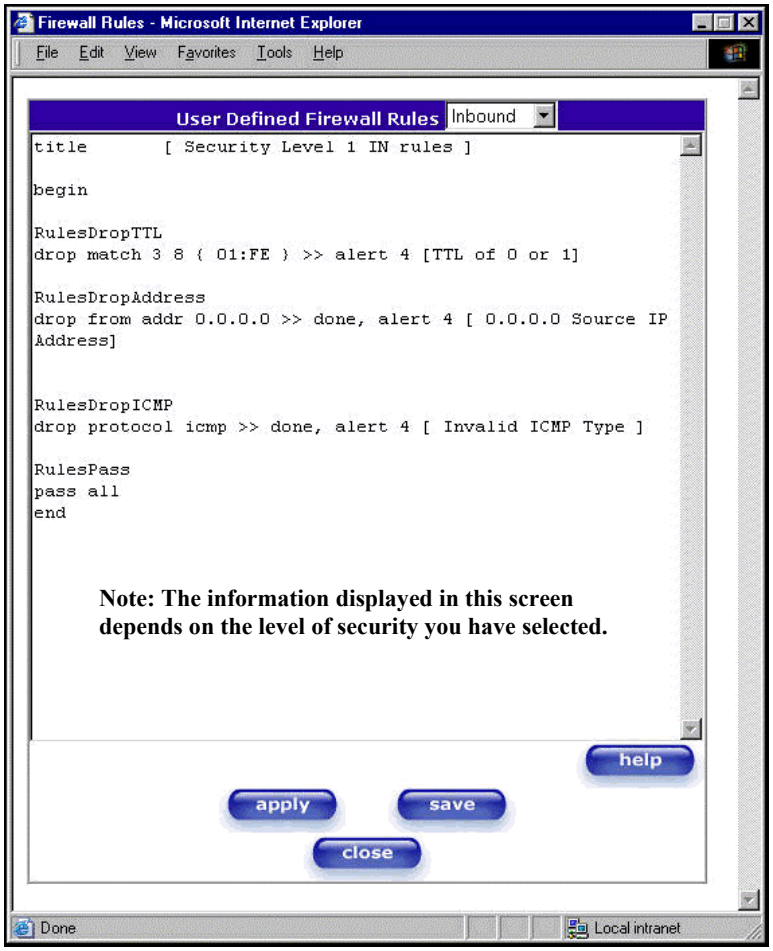
IMPORTANT: Westell recommends that you do not change the settings in the **User Defined Firewall Rules** screen. If you need to reset VersaLink to factory default settings, push the reset button on the rear of VersaLink.



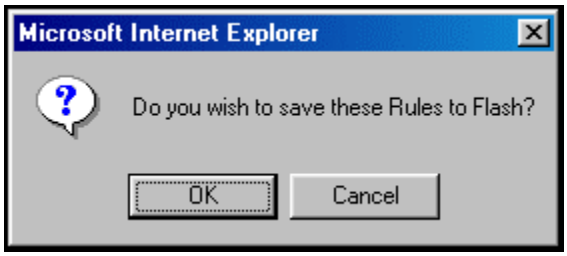
If you clicked **Apply** in the **User Define Firewall Rules** screen, the following pop-up screen will be displayed. Click **OK** to apply the rules and to switch your security level to "Custom." If you click **cancel,** the change will not take effect.

If you clicked **OK** in the pop-up screen, the following screen will be displayed. Click **save** to save to continue.

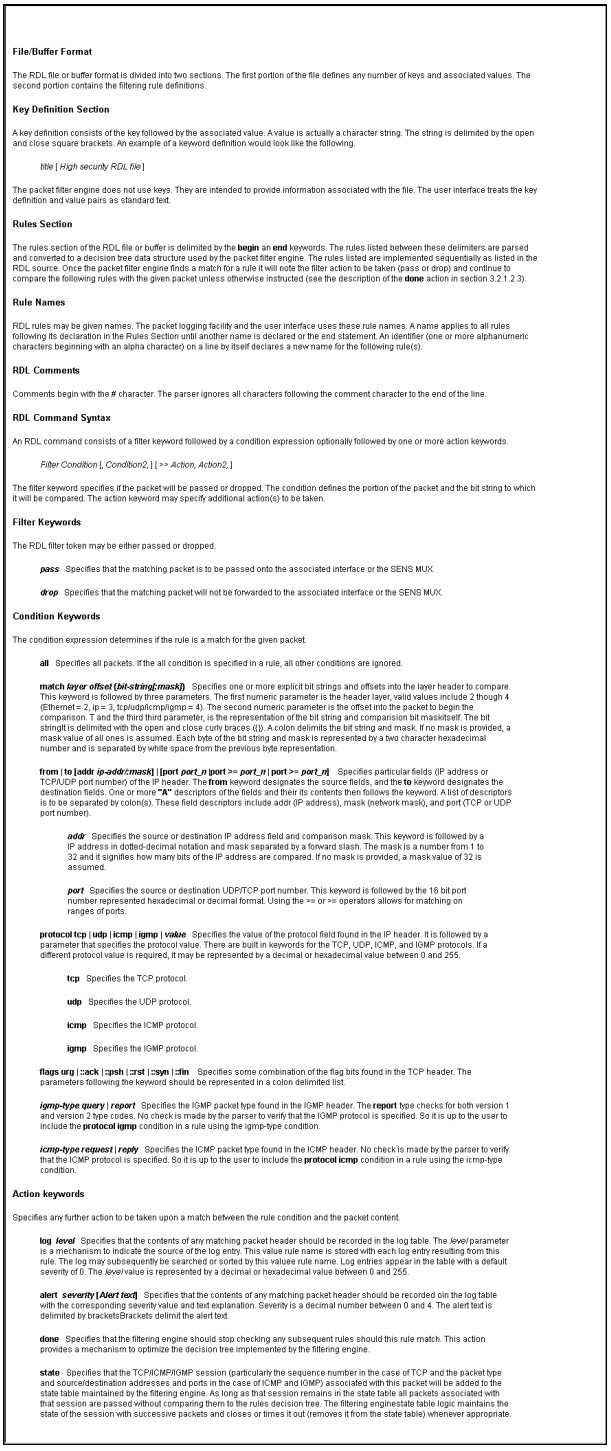
IMPORTANT: Westell recommends that you do not change the settings in the **User Defined Firewall Rules** screen. If you need to reset VersaLink to factory default settings, push the reset button on the rear of VersaLink.


Firewall Rules - Microsoft Internet Explorer
File Edit View Favorites Tools Help
User Defined Firewall Rules
Inbound
title [Security Level 1 IN rules]
begin
RulesDropTTL
drop match 3 8 (01:FE) >> alert 4 [TTL of 0 or 1]
RulesDropAddress
drop from addr 0.0.0.0 >> done, alert 4 [0.0.0.0 Source IP Address]
RulesDropICMP
drop protocol icmp >> done, alert 4 [Invalid ICMP Type]
RulesPass
pass all
end
Note: The information displayed in this screen depends on the level of security you have selected.
help
apply
save
close
Done
Local intranet

If you clicked **save**, the following pop-up screen will be displayed. Click **OK** when asked **"Do you wish to save these Rules to Flash?"** The new firewall settings will be saved.. If you click **Cancel,** your new firewall settings will not be saved.



If you select **Help** in the screen labeled **User Defined Firewall Rules**, the following screen will be displayed. This screen gives a detailed explanation of the Firewall Rules.



File/Buffer Format

The RDL file or buffer format is divided into two sections. The first portion of the file defines any number of keys and associated values. The second portion contains the filtering rule definitions.

Key Definition Section

A key definition consists of the key followed by the associated value. A value is actually a character string. The string is delimited by the open and close square brackets. An example of a keyword definition would look like the following.

title [High security RDL file]

The packet filter engine does not use keys. They are intended to provide information associated with the file. The user interface treats the key definition and value pairs as standard text.

Rules Section

The rules section of the RDL file or buffer is delimited by the **begin** an **end** keywords. The rules listed between these delimiters are parsed and converted to a decision tree data structure used by the packet filter engine. The rules listed are implemented sequentially as listed in the RDL source. Once the packet filter engine finds a match for a rule it will note the filter action to be taken (pass or drop) and continue to compare the following rules with the given packet unless otherwise instructed (see the description of the **done** action in section 3.2.1.2.3).

Rule Names

RDL rules may be given names. The packet logging facility and the user interface uses these rule names. A name applies to all rules following its declaration in the Rules Section until another name is declared or the end statement. An identifier (one or more alphanumeric characters beginning with an alpha character) on a line by itself declares a new name for the following rule(s).

RDL Comments

Comments begin with the # character. The parser ignores all characters following the comment character to the end of the line.

RDL Command Syntax

An RDL command consists of a filter keyword followed by a condition expression optionally followed by one or more action keywords.

Filter Condition [, Condition2,] [=> Action, Action2,]

The filter keyword specifies if the packet will be passed or dropped. The condition defines the portion of the packet and the bit string to which it will be compared. The action keyword may specify additional action(s) to be taken.

Filter Keywords

The RDL filter token may be either passed or dropped.

pass Specifies that the matching packet is to be passed onto the associated interface or the SENS MUX.

drop Specifies that the matching packet will not be forwarded to the associated interface or the SENS MUX.

Condition Keywords

The condition expression determines if the rule is a match for the given packet.

all Specifies all packets. If the all condition is specified in a rule, all other conditions are ignored.

match *layer offset {bit-string[:mask]}* Specifies one or more explicit bit strings and offsets into the layer header to compare. This keyword is followed by three parameters. The first numeric parameter is the header layer, valid values include 2 though 4 (Ethernet = 2, ip = 3, tcp/udp/icmp/igmp = 4). The second numeric parameter is the offset into the packet to begin the comparison. T and the third third parameter, is the representation of the bit string and comparision bit maskitself. The bit stringIt is delimited with the open and close curly braces ({}). A colon delimits the bit string and mask. If no mask is provided, a mask value of all ones is assumed. Each byte of the bit string and mask is represented by a two character hexadecimal number and is separated by white space from the previous byte representation.

from | to [addr *ip-addr:mask*] | [port *port_n* |port >= *port_n* | port >= *port_n*] Specifies particular fields (IP address or TCP/UDP port number) of the IP header. The **from** keyword designates the source fields, and the **to** keyword designates the destination fields. One or more **"A"** descriptors of the fields and their its contents then follows the keyword. A list of descriptors is to be separated by colon(s). These field descriptors include addr (IP address), mask (network mask), and port (TCP or UDP port number).

addr Specifies the source or destination IP address field and comparison mask. This keyword is followed by a IP address in dotted-decimal notation and mask separated by a forward slash. The mask is a number from 1 to 32 and it signifies how many bits of the IP address are compared. If no mask is provided, a mask value of 32 is assumed.

port Specifies the source or destination UDP/TCP port number. This keyword is followed by the 16 bit port number represented hexadecimal or decimal format. Using the >= or =< operators allows for matching on ranges of ports.

protocol tcp | udp | icmp | igmp | *value* Specifies the value of the protocol field found in the IP header. It is followed by a parameter that specifies the protocol value. There are built in keywords for the TCP, UDP, ICMP, and IGMP protocols. If a different protocol value is required, it may be represented by a decimal or hexadecimal value between 0 and 255.

tcp Specifies the TCP protocol.

udp Specifies the UDP protocol.

icmp Specifies the ICMP protocol.

igmp Specifies the IGMP protocol.

flags urg | □ack | □psh | □rst | □syn | □fin Specifies some combination of the flag bits found in the TCP header. The parameters following the keyword should be represented in a colon delimited list.

igmp-type query | report Specifies the IGMP packet type found in the IGMP header. The **report** type checks for both version 1 and version 2 type codes. No check is made by the parser to verify that the IGMP protocol is specified. So it is up to the user to include the **protocol igmp** condition in a rule using the igmp-type condition.

icmp-type request | reply Specifies the ICMP packet type found in the ICMP header. No check is made by the parser to verify that the ICMP protocol is specified. So it is up to the user to include the **protocol icmp** condition in a rule using the icmp-type condition.

Action keywords

Specifies any further action to be taken upon a match between the rule condition and the packet content.

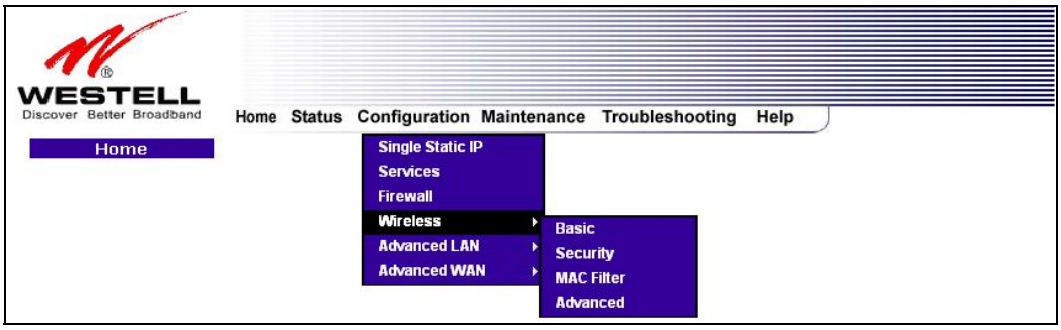
log *level* Specifies that the contents of any matching packet header should be recorded in the log table. The *level* parameter is a mechanism to indicate the source of the log entry. This value rule name is stored with each log entry resulting from this rule. The log may subsequently be searched or sorted by this valuee rule name. Log entries appear in the table with a default severity of 0. The *level* value is represented by a decimal or hexadecimal value between 0 and 255.

alert *severity [Alert text]* Specifies that the contents of any matching packet header should be recorded oin the log table with the corresponding severity value and text explanation. Severity is a decimal number between 0 and 4. The alert text is delimited by bracketsBrackets delimit the alert text.

done Specifies that the filtering engine should stop checking any subsequent rules should this rule match. This action provides a mechanism to optimize the decision tree implemented by the filtering engine.

state Specifies that the TCP/ICMP/IGMP session (particularly the sequence number in the case of TCP and the packet type and source/destination addresses and ports in the case of ICMP and IGMP) associated with this packet will be added to the state table maintained by the filtering engine. As long as that session remains in the state table all packets associated with that session are passed without comparing them to the rules decision tree. The filtering enginestate table logic maintains the state of the session with successive packets and closes or times it out (removes it from the state table) whenever appropriate.

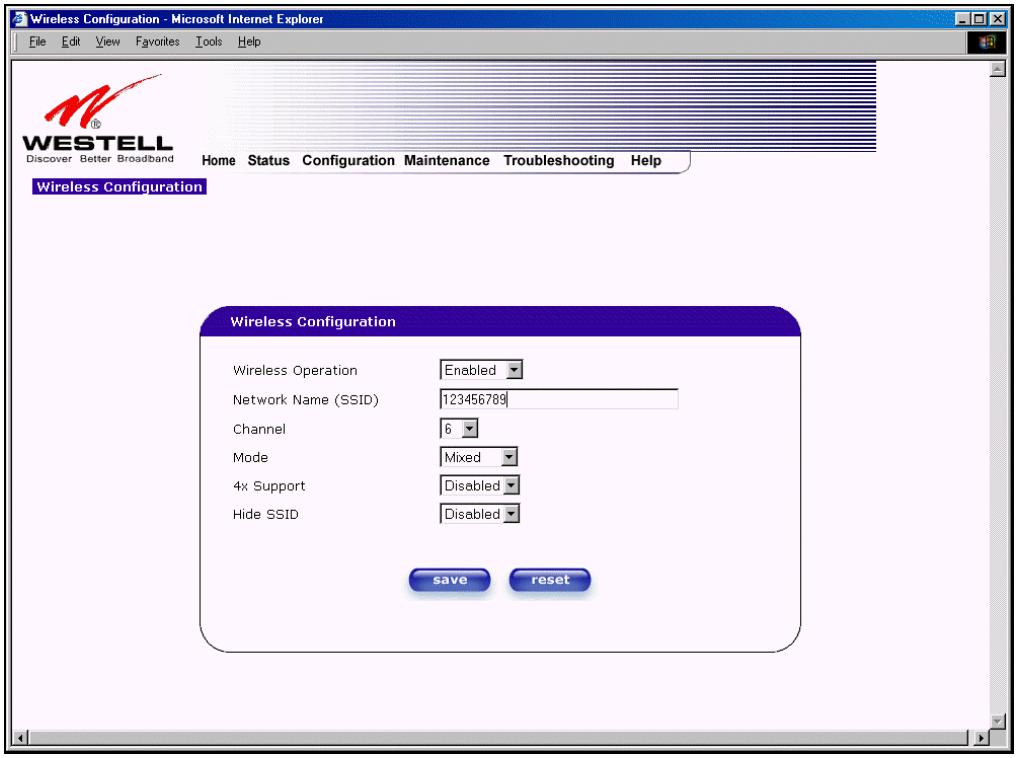
13.4 Wireless Configuration



13.4.1 Wireless Basic

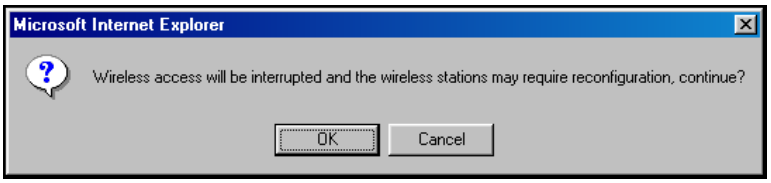
The following fields will be displayed if you select **Wireless** > **Basic** from the **Configuration** menu.

IMPORTANT: If you are connecting to VersaLink via a wireless network adapter, the Service Set ID (SSID) must be the same for both the Westell VersaLink and your PC's wireless network adapter. The default SSID for VersaLink is the serial number of the unit (located below the bar code on the bottom of the unit and also on the Westell shipping carton). Locate and run the utility software provided with your PC's Wireless network adapter and enter the SSID value. The PC's wireless network adapter must be configured with the SSID (in order to communicate with VersaLink) before you begin VersaLink's account setup and configuration procedures. For privacy, you should change the **Network Name (SSID)** value in the **Wireless Configuration** screen to your desired value.



Wireless Configuration	
Wireless Operation	Factory Default = Enabled. When disabled, no stations will be able to connect to the VersaLink.
Network Name (SSID)	This string, (32 characters or less) is the name associated with the modem. To connect to the modem, the SSID on a station must match the SSID on the modem.
Channel	Factory Default = 6. The modem transmits and receives data on this channel. The number of channels to choose from is pre-programmed into the modem. Station cards do not have to be set to the same channel as the AP; the stations scan all channels, and look for an AP to connect to.
Mode	Factory Default = Mixed. This setting allows station to communicate with VersaLink. Possible Responses: Mixed: Station using any of the 802.11b, 802.11b+, and 802.11g rates can communicate with VersaLink. 11b only: Communication with VersaLink is limited to 802.11b 11b+: Stations using any of the 802.11b and 802.11b+ rates can communicate with VersaLink. 11g only: Communication with VersaLink is limited to 802.11g
4x Support	Factory Default = Disabled. When selected, this enables/disables the 4X option. If enabled, 4X support provides additional algorithms for increased throughput. The station cards must also support this option.
Hide SSID	Factory Default = Disabled. If Enabled, VersaLink will not broadcast the SSID. Stations must configure the SSID to match the Network Name (SSID) to connect to VersaLink.

If you click **save** in the **Wireless Configuration** screen, the following pop-up will be displayed. Click **OK** to save the settings.

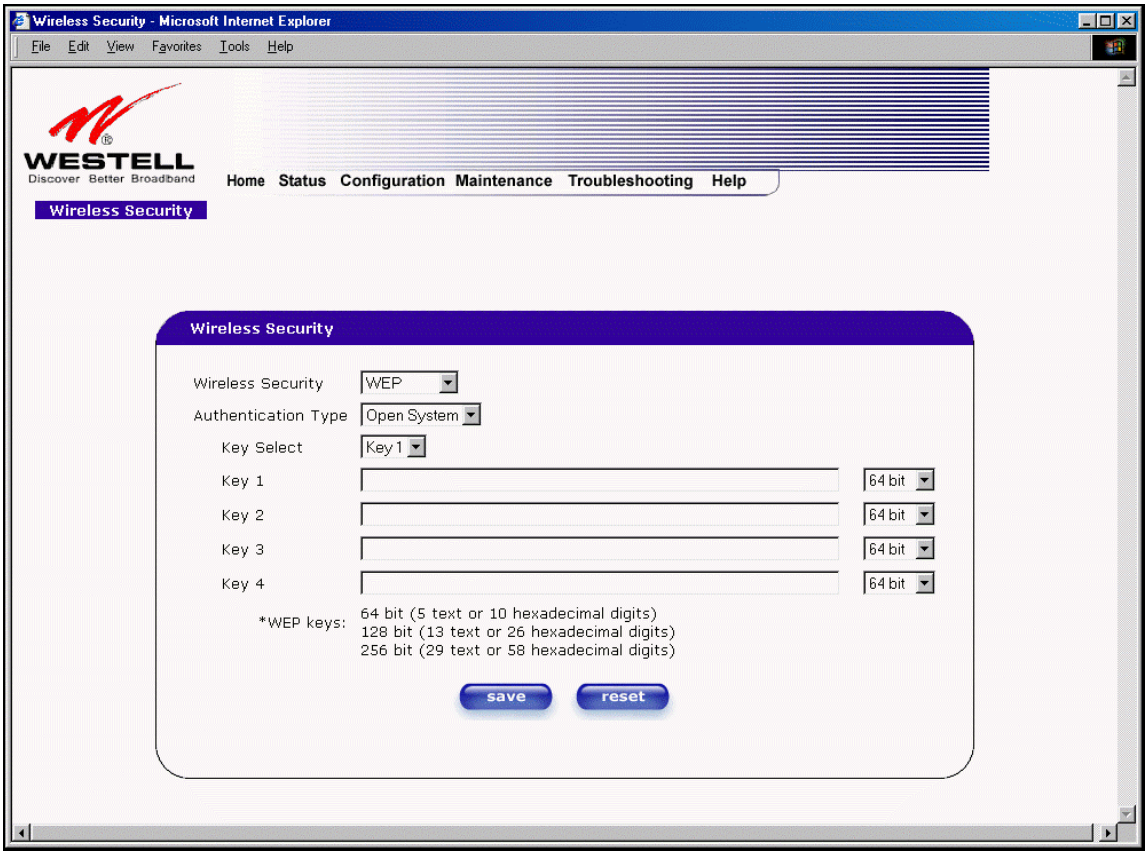

Microsoft Internet Explorer
Wireless access will be interrupted and the wireless stations may require reconfiguration, continue?
OK
Cancel

13.4.2 Wireless Security

The following screen will be displayed if you select **Wireless** > **Security** from the **Configuration** menu.

To configure your wireless security settings, select the desired security option from the **Wireless Security** drop-down menu. If you change any settings in this screen, be sure to click **save** to allow the settings to take effect.

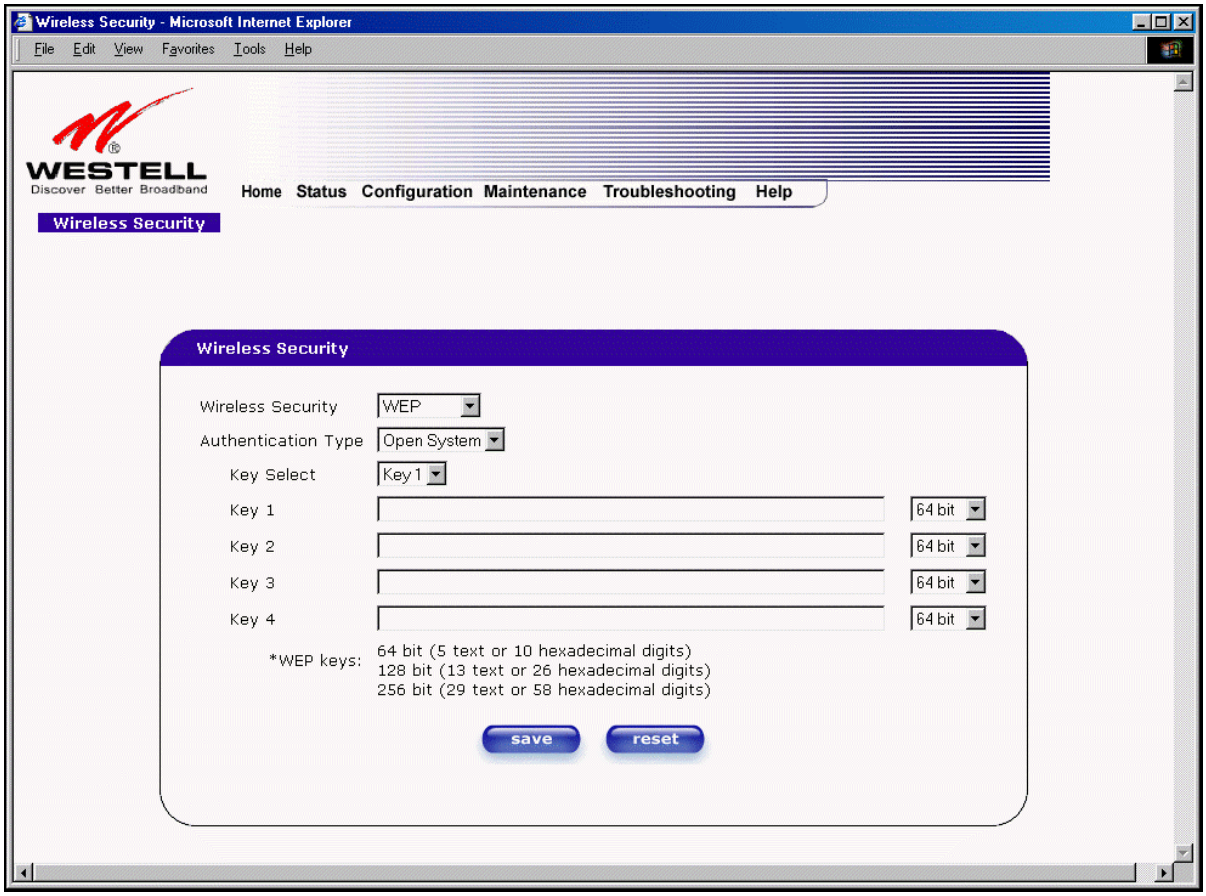
IMPORTANT: Client PCs can use any Wireless Fidelity (Wi-Fi) 802.11b/g certified card to communicate with VersaLink; however, the Wireless card and VersaLink must use the same security code type. **If you use WPA-PSK or WEP wireless security, you must configure your computer's wireless adapter with the security code.**


Wireless Security - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Wireless Security
Wireless Security
Wireless Security WEP
Authentication Type Open System
Key Select Key 1
Key 1 64 bit
Key 2 64 bit
Key 3 64 bit
Key 4 64 bit
*WEP keys: 64 bit (5 text or 10 hexadecimal digits)
128 bit (13 text or 26 hexadecimal digits)
256 bit (29 text or 58 hexadecimal digits)
save
reset

13.4.2.1 Enabling WEP security

If you selected **WEP** (the factory default setting) from the **Wireless Security** drop-down menu, the following screen will be displayed. After you have entered the appropriate values in the fields provided, click **save** to save the settings.

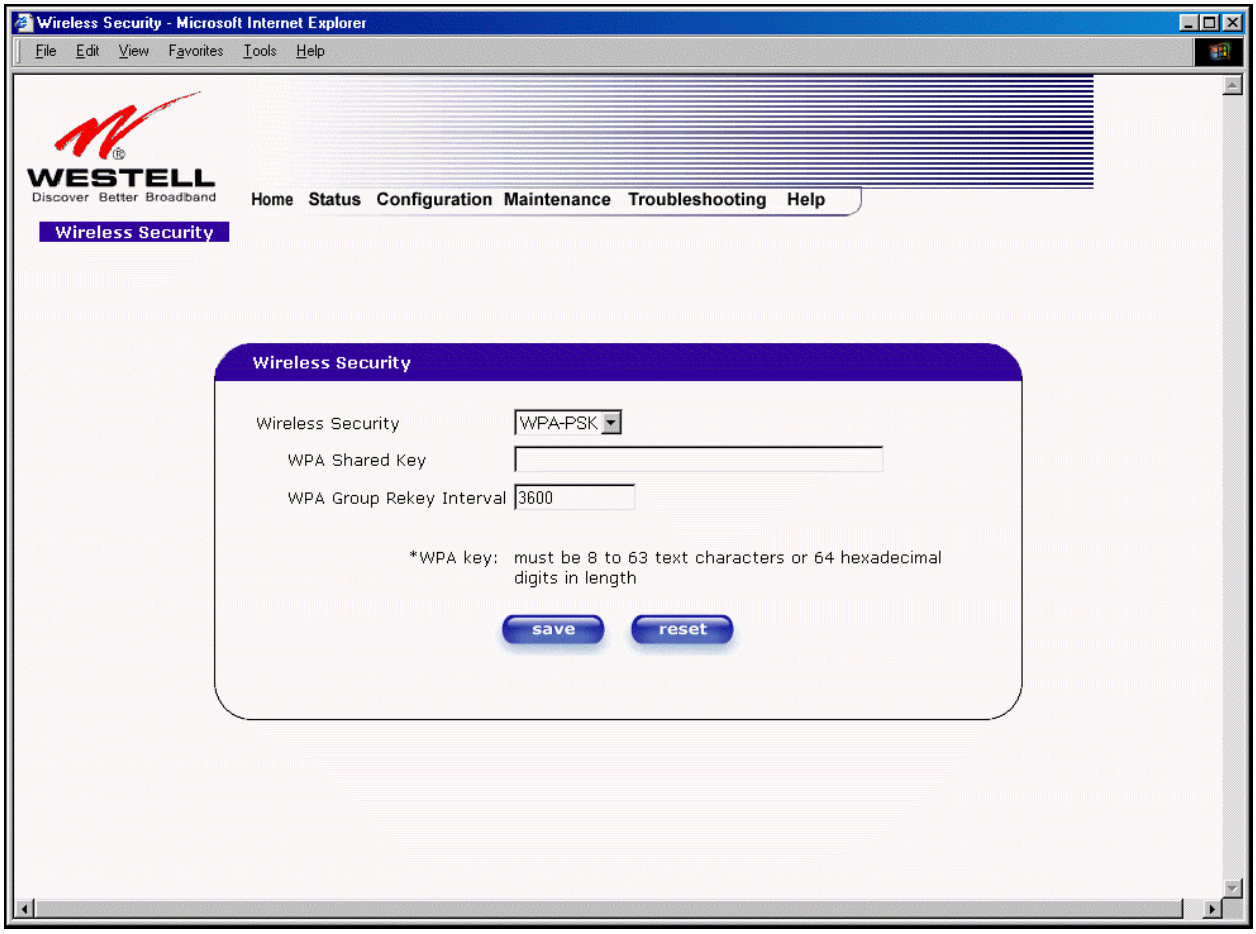
NOTE: The WEP key must be 64 bit (5 text characters or 10 hexadecimal digits in length) or 128 bit (13 text characters or 26 hexadecimal characters in length).


Wireless Security - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Wireless Security
Wireless Security
Wireless Security WEP
Authentication Type Open System
Key Select Key 1
Key 1 64 bit
Key 2 64 bit
Key 3 64 bit
Key 4 64 bit
*WEP keys: 64 bit (5 text or 10 hexadecimal digits)
128 bit (13 text or 26 hexadecimal digits)
256 bit (29 text or 58 hexadecimal digits)
save reset

Wireless Security (WEP)	
Wireless Security	Factory Default = WEP Possible Response: Disabled: Wireless security will be disabled on the VersaLink. WPA-PSK: Selecting this will enable you to set up WPA-PSK security on the VersaLink. WEP: Selecting this will enable you to set up WEP security on the VersaLink. The AP card supports 64-bit, 128-bit, or 256-bit WEP encryption. If WEP is selected, any station can connect to the AP (as long as its SSID matches the AP SSID). IF WEP is enabled, the risk of someone nearby accessing the AP is minimized.
Authentication Type	Factory Default = Open System Possible Response: Open System: Open System authentication is the default selection. Shared Key: To use Shared Key authentication, WEP must be enabled, and a valid WEP key must be present. Enabling WEP does not force the use of Shared Key authentication. It is permissible to have WEP enabled and still use Open System authentication.
Key Select	If selected, the WEP Key is treated as a string of text characters, and the number of characters must

	be either 5 (for 64-bit encryption) or 13 (for 128-bit encryption) or 29 (for 256-bit encryption). If not selected, the WEP key is treated as a string of hexadecimal characters, and the number of characters must be either 10 (for 64-bit encryption), 26 (for 128-bit encryption), or 58 (for 256-bit encryption). The only allowable hexadecimal characters are 0-9 and A-F. NOTE: The WEP key must be the same value and type for both VersaLink and the wireless network adapter. "Pass Phrase" is not the same as "text" and should not be used.

If you select **WPA-PSK** from the **Wireless Security** drop-down menu, the following screen will be displayed. Enter your **WPA Shared Key** and **WPA Group Rekey Interval** in the fields provided. Click **save** to save the settings.


Wireless Security - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Wireless Security
Wireless Security
Wireless Security WPA-PSK
WPA Shared Key
WPA Group Rekey Interval 3600
*WPA key: must be 8 to 63 text characters or 64 hexadecimal digits in length
save
reset

Wireless Security	
Wireless Security	Factory Default = WEP. Possible Response: Disabled: Wireless security will be disabled on the VersaLink. WPA-PSK: Selecting this will enable you to set up WPA-PSK security on the VersaLink. WEP: Selecting this will enable you to set up WEP security on the VersaLink. The AP card supports 64-bit, 128-bit, or 256-bit WEP encryption. If WEP is selected, any station can connect to the AP (as long as its SSID matches the AP SSID). If wireless security is disabled, the risk of someone nearby accessing the AP is maximized.
WPA Shared Key	This is a passphrase (also called a shared secret) that must be entered in both the wireless router and the wireless client. This shared secret can be between 8 to 63 text characters (or 64

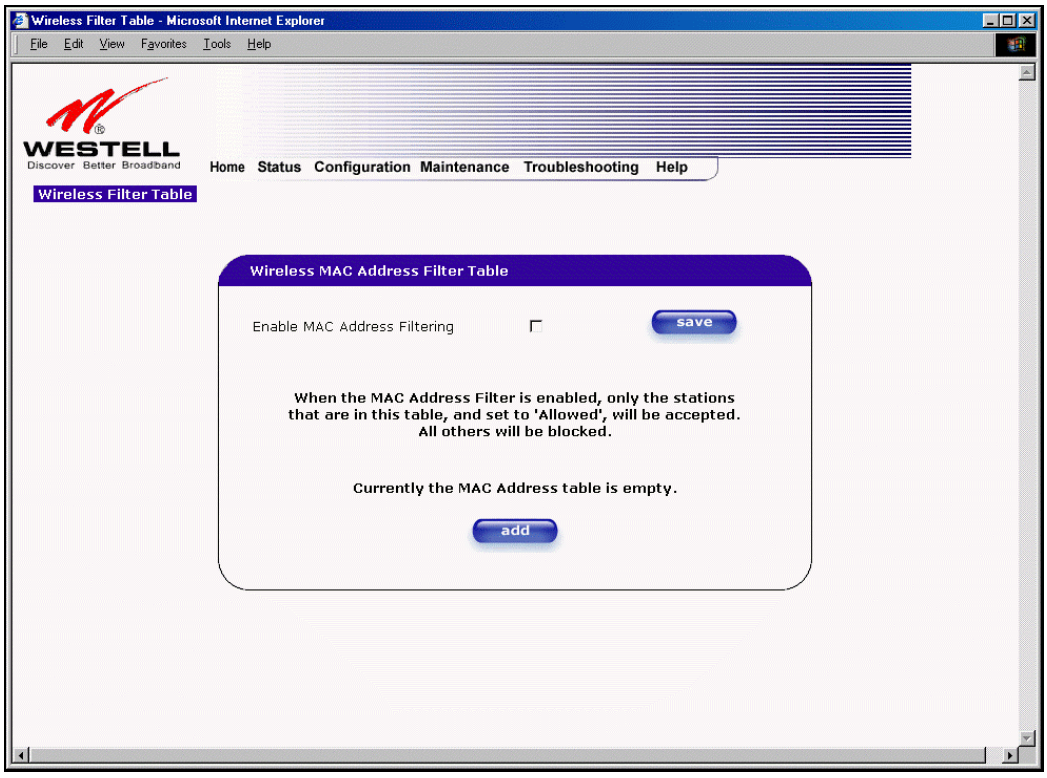
	hexadecimal characters) and can include special characters and spaces. The WPA Shared Key should be a random sequence of either keyboard characters (upper and lowercase letters, numbers, and punctuation), at least 20 characters long, or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. The more random your WPA Shared Key, the safer it is to use.
WPA Group Rekey Interval	Factory Default = 3600. The number of seconds between rekeying the WPA group key. A zero "0" means that rekeying is disabled.

13.4.3 Wireless Media Access Controller (MAC) Filter Table

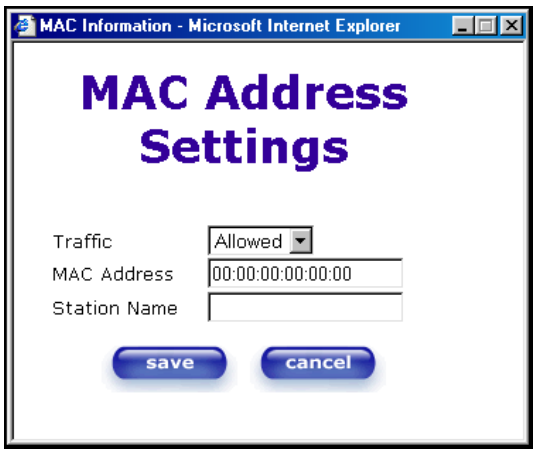
The following screen will be displayed if you select **MAC Filter > Wireless** from the **Configuration** menu.

NOTE: When the MAC Address is enabled, only the stations that are in this table, and set to "Allowed," will be accepted. All other stations will be blocked.

To enable MAC Address filtering, click the check box adjacent to **Enable MAC Address Filtering**. A check mark will appear in the box. Next, click **save** to save the setting. To add or edit a MAC Address setting, click the **add** button.

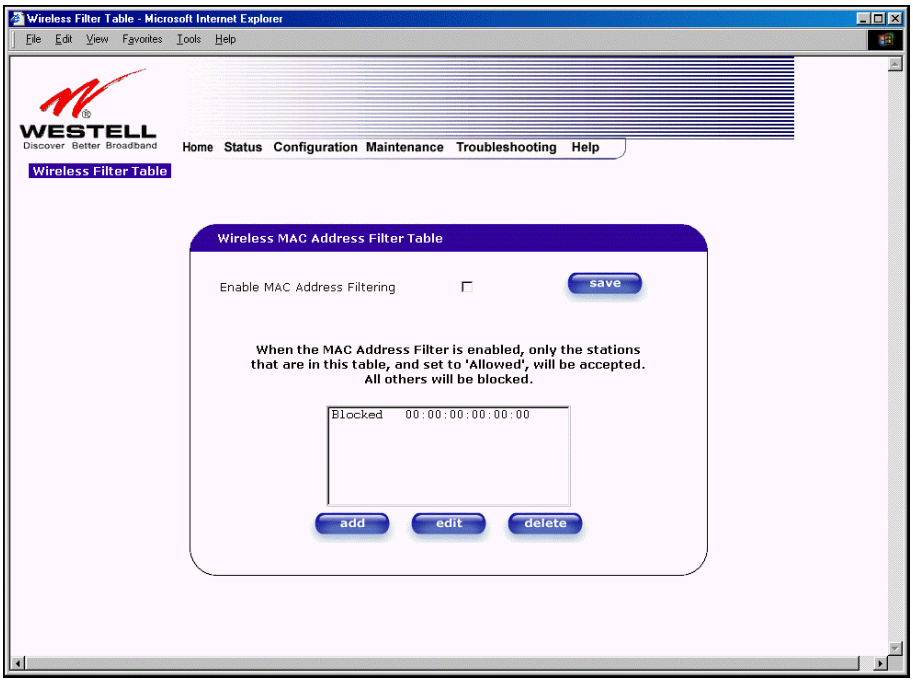

Wireless Filter Table - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Wireless Filter Table
Wireless MAC Address Filter Table
Enable MAC Address Filtering
save
When the MAC Address Filter is enabled, only the stations that are in this table, and set to 'Allowed', will be accepted. All others will be blocked.
Currently the MAC Address table is empty.
add

If you clicked **add** in the preceding screen, the following screen will be displayed. Enter and/or select the appropriate values for your MAC address settings, and then click **save** to save the settings. Click **cancel** if you do not want to save the changes.



Traffic	Allowed: When the MAC Filter is enabled, only stations in the MAC Filter Table (which are set to "Allowed") will have access to the modem. Blocked: This allows the station to remain in the table, but no access to the VersaLink is allowed.
MAC Address	The MAC address assigned to the station to which you want to allow access.
Station Name	The station name or description to which the MAC address is assigned. This is an optional field that is useful in identifying the station.

After you have entered your MAC address settings and clicked **save**, the following screen will be displayed. Next, click the **Enable MAC Address Filtering** box (a check mark will appear in the box). Click **save** to save the settings.

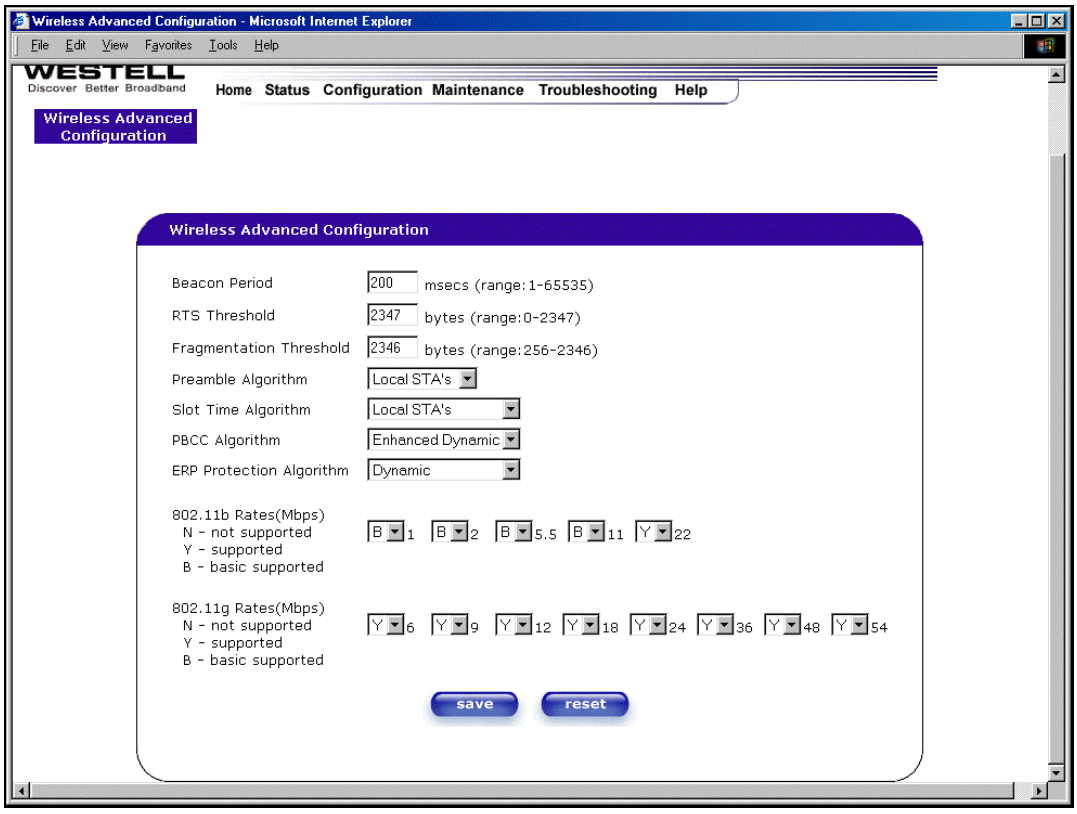

Wireless Filter Table - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Wireless Filter Table
Wireless MAC Address Filter Table
Enable MAC Address Filtering
save
When the MAC Address Filter is enabled, only the stations that are in this table, and set to 'Allowed', will be accepted. All others will be blocked.
Blocked 00:00:00:00:00:00
add
edit
delete

If you clicked **save**, the following pop-up screen will be displayed. Click **OK** to continue.

NOTE: If you make changes to your wireless settings and then save the settings, wireless access will be interrupted for all wireless devices that are connected to your VersaLink.

13.4.4 Wireless Advanced Configuration

The following screen will be displayed if you select **Wireless > Advanced** from the **Configuration** menu.


Wireless Advanced Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Wireless Advanced Configuration
Wireless Advanced Configuration
Beacon Period 200 msecs (range: 1-65535)
RTS Threshold 2347 bytes (range: 0-2347)
Fragmentation Threshold 2346 bytes (range: 256-2346)
Preamble Algorithm Local STA's
Slot Time Algorithm Local STA's
PBCC Algorithm Enhanced Dynamic
ERP Protection Algorithm Dynamic
802.11b Rates(Mbps)
N - not supported
Y - supported
B - basic supported
B 1 B 2 B 5.5 B 11 Y 22
802.11g Rates(Mbps)
N - not supported
Y - supported
B - basic supported
Y 6 Y 9 Y 12 Y 18 Y 24 Y 36 Y 48 Y 54
save
reset

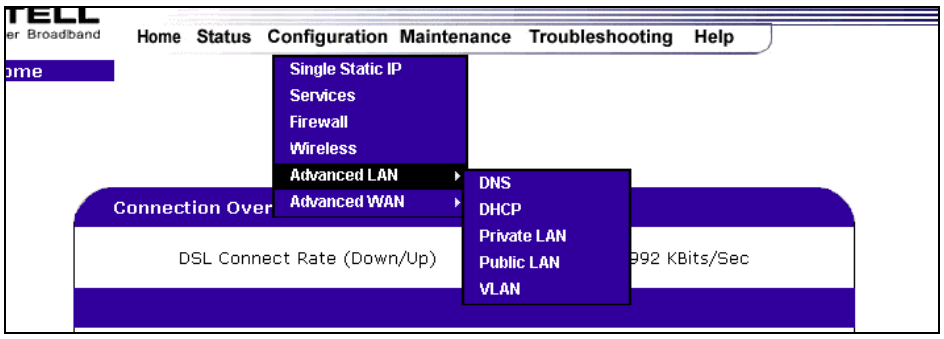
Beacon Period	The time interval between beacon frame transmissions. Beacons contain rate and capability information. Beacons received by stations can be used to identify the access points in the area.
RTS Threshold	RTS/CTS handshaking will be performed for any data or management MPDU containing a number of bytes greater than the threshold. If this value is larger than the MSDU size (typically set by the fragmentation threshold), no handshaking will be performed. A value of zero will enable handshaking for all MPDUs.

Fragmented Threshold	Any MSDU or MMPDU larger than this value will be fragmented into an MPDU of the specified size.
Preamble Algorithm	Factory Default = Local STA's Possible Responses: Always Long: Transmissions are done using the long preamble algorithm. Always Short: Transmissions are done using the short preamble algorithm. Local STA's: If all associated stations support short preamble, then the short preamble algorithm is used. Otherwise, the long preamble algorithm is used.
Slot Time Algorithm	Factory Default = Local STA's Possible Response: Always Off: Transmissions are done using a 20 usec slot time. Always ON: Transmissions are done using a usec slot time (SST). Local STA's: If all associated stations support SST, then the 9 usec slot time is used. Otherwise, the 20 uses slot time is used. Enhanced Dynamic: Similar to Local STA's, with the following extension: If associated stations that do not support SST do not transmit for a period of time, the 9 usec slot time is used.
PBCC Algorithm	Factory Default = Enhanced Dynamic Possible Response: Always Off: PBCC is not used, operation at 22 Mbps is not possible. Always ON: PBCC is used. Local STA's: If all associated stations support PBCC, then PBCC is used. Otherwise, PBCC is not used. Dynamic: Similar to local STA's with the following extension: PBCC setting is also dependent on Beacon frames from overlapping BSS. If Beacon frames are received that do not support PBCC, then PBCC is not used. Enhanced Dynamic: Similar to Dynamic with the following extension: If associated stations that do not support PBCC do not transmit for a period of time, then PBCC is not used.
ERP Protection Algorithm	Factory Default = Dynamic Possible Response: Always Off: ERP is not used Always ON: ERP is used. Local STA's: If there are any associated stations than do not support ERP, a protection algorithm is used to prevent contention. Dynamic: Similar to local STA's with the following extension: The ERP protection setting is also dependent on Beacon frames from overlapping BSS. IF Beacon frames are received that indicate ERP is not supported, then a protection algorithm is used. Enhanced Dynamic: Similar to Dynamic with the following extension: If associated stations that do not support ERP do not transmit for a period of time, then protection algorithm is not used.
802.11b Rates (Mbps) 802.11g Rates (Mbps)	These are the allowable communication rates that VersaLink will attempt to use. The rates are also broadcast within the connection protocol as the rates supported by VersaLink.

13.5 Advanced LAN

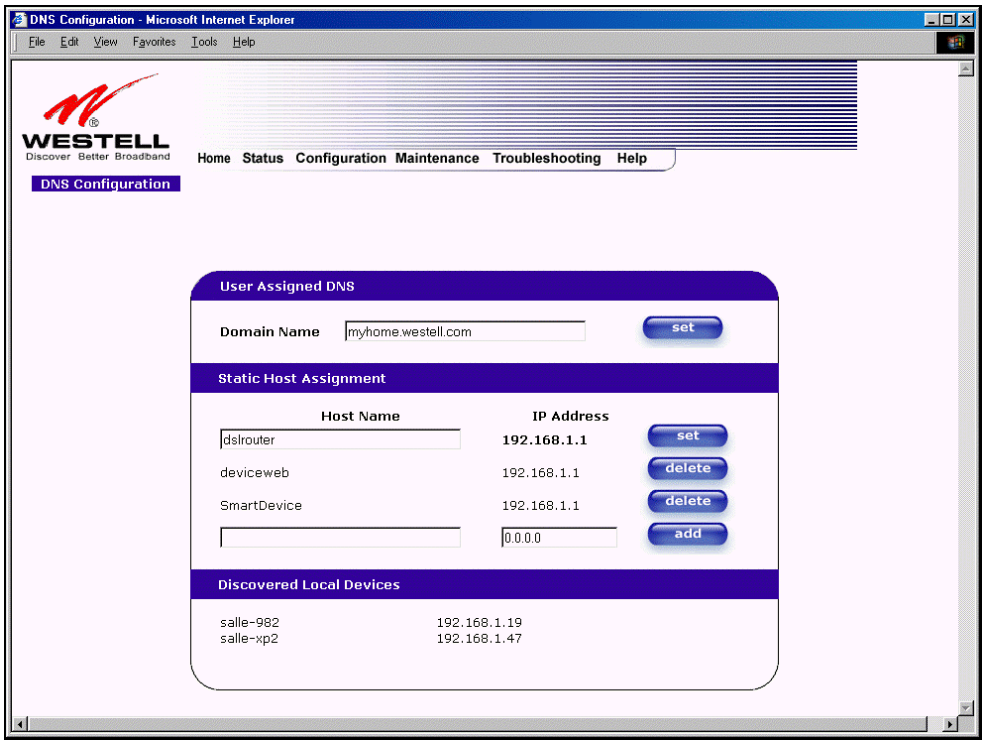
This section explains the configurable features of VersaLink that are available if you select **Advanced LAN** from the **Configuration** menu.

NOTE: If VersaLink is configured for **ETHERNET PORT 1**, **VLAN** will not be displayed. You must configure VersaLink for **DSLATM PORT** to access **VLAN** in the **Advanced LAN** drop-down menu. Refer to section 13.6.2.2 for details.



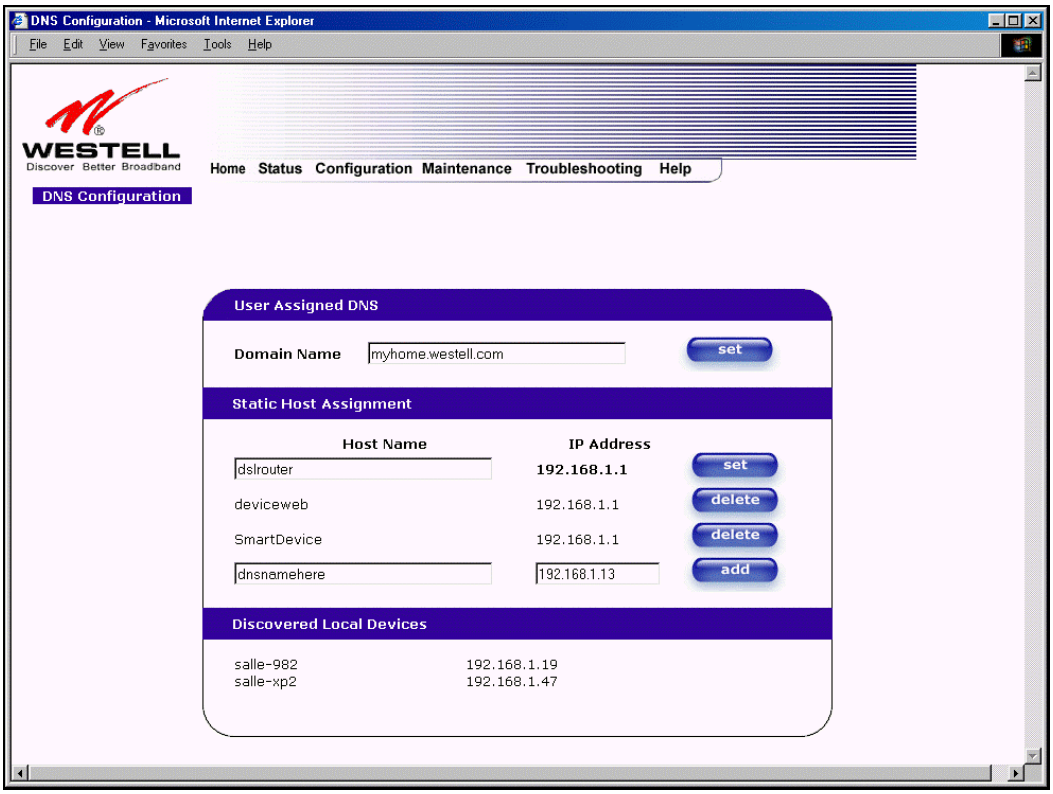
13.5.1 DNS Configuration

The following screen will be displayed if you select **DNS** from the **Advanced LAN** menu.

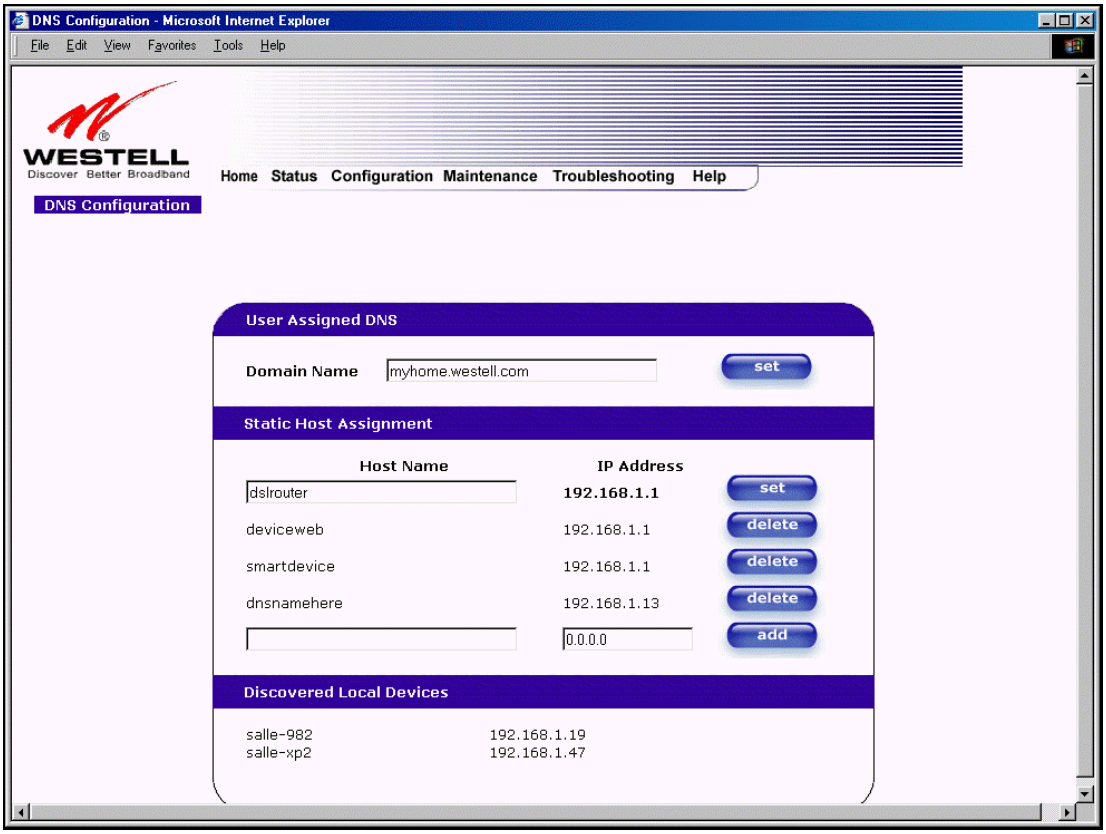


User Assigned DNS	
Domain Name NOTE: Some ISP's may require the name for identification purposes.	This field allows you to enter a Domain Name for VersaLink. To add a Domain Name, in the field under User Assigned DNS, type in your new domain name and click **Set.**
Static Host Assignment	
Host Name	This field allows you to enter a HOST name for VersaLink. To add a new Host name, in the field under Static Host Assignment, type in the Host Name and the IP address and click **Set.**
IP Address	Displays the IP address that is assigned to the Host Name.
Discover Local Devices	
This field displays a list of the computers on the LAN that were assigned a DHCP Address. The DNS name and IP address entry of each discovered device is displayed. (NOTE: The values in this field will be displayed barring any propagation delays. If 'No Discovered Devices' is displayed, manually refresh the screen.)	

If you want to add a new Host Name and IP address to your DNS server, type the **Host Name** and **IP Address** in the fields provided in the **Static Host Assignment** section. Then, click **add** to continue.



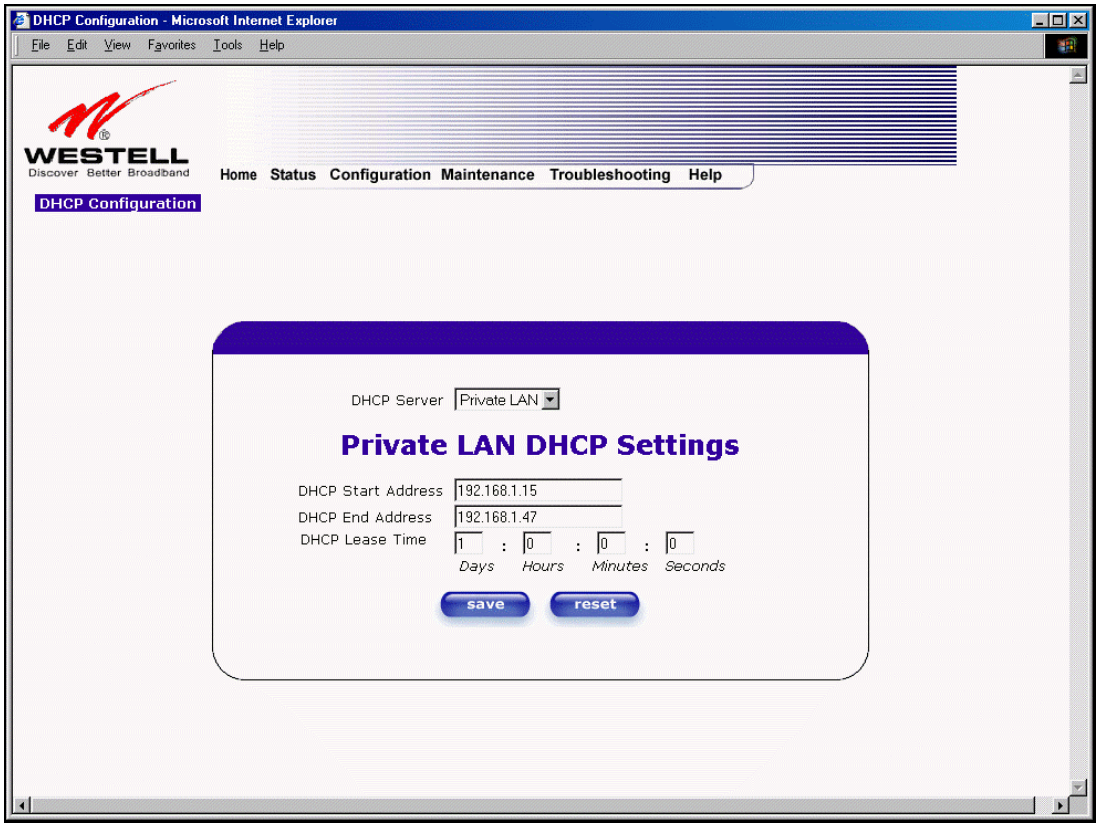
If you clicked **add**, the following screen will be displayed. This screen shows that the **Host Name** and **IP Address** have been added to the DNS server. If you want to delete a static host assignment, click the **delete** button adjacent to the Host Name and IP address that you want to delete.



13.5.2 DHCP Configuration (Private LAN)

The following screen will be displayed if you select **Advanced LAN > DHCP** from the **Configuration** menu.

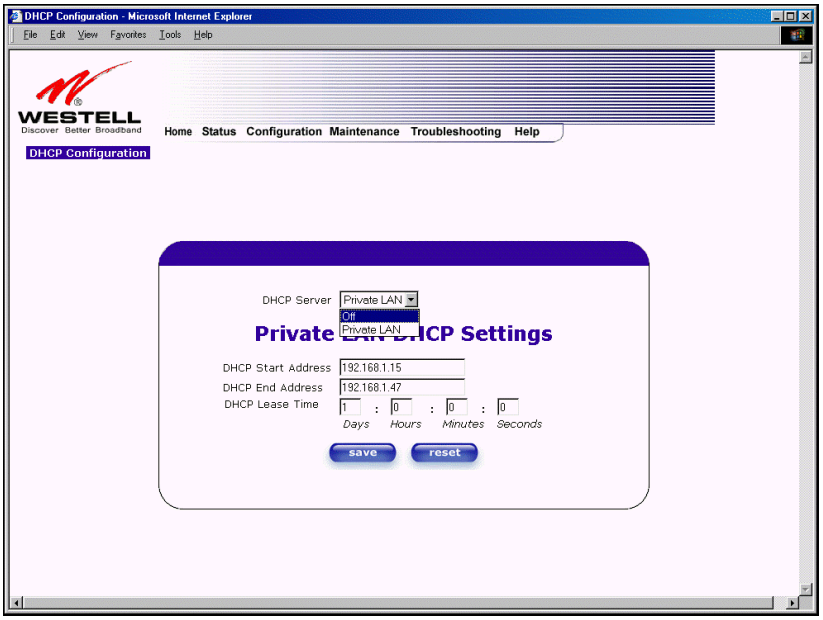
IMPORTANT: These settings are provided by your ISP. Please do not change these settings unless you are instructed to do so.


DHCP Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
DHCP Configuration
DHCP Server Private LAN
Private LAN DHCP Settings
DHCP Start Address 192.168.1.15
DHCP End Address 192.168.1.47
DHCP Lease Time 1 : 0 : 0 : 0
Days Hours Minutes Seconds
save reset

DHCP Server	This setting allows VersaLink to automatically assign IP addresses to local devices connected on the LAN. Westell advises setting this to enabled for the private LAN. Off = DHCP Server is disabled Private LAN = DHCP addresses will be saved into the Private LAN configuration. Public LAN = DHCP addresses will be saved into the Public LAN configuration. This option is only available if the Public LAN DHCP server is enabled.
DHCP Start Address	Factory Default = 192.168.1.15 This field displays the first IP address that the DHCP server will provide. The DHCP Start Address must be within the IP address and lower than the DHCP End Address. You may use any number from 0 to 254 in this address.
DHCP End Address	Factory Default = 192.168.1.47 This field displays the last IP address that the DHCP server will provide. The DHCP End Address must be within the IP address and higher than the DHCP Start Address. You may use any number from 0 to 254 in this address.
DHCP Lease Time	Factory Default = 01:00:00:00 Displays the amount of time the provided addresses will be valid, after which the DHCP client will usually re-submit a request. NOTE: This value must be greater than 10 seconds. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.

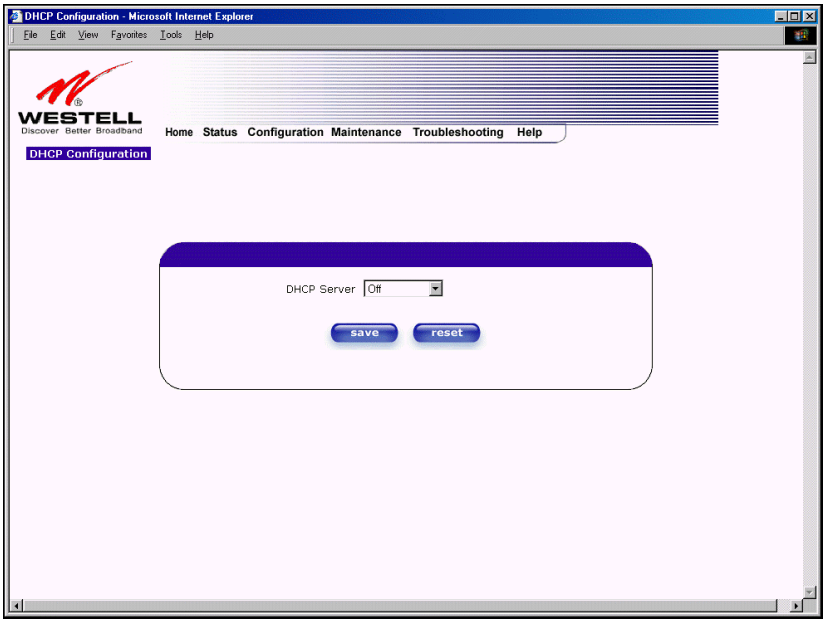
13.5.3 Disabling the DHCP Server

To disable the DHCP server, select **Off** from the **DHCP Server** drop-down menu.



If you selected **Off** from drop-down menu, the following screen will be displayed automatically. Now click **save** to save the settings. If you click **reset**, the screen will refresh and the previously saved settings will be remain active.

IMPORTANT: Whenever you change the DHCP Server settings, the screen will display the changes; however, you must click **save** to allow the changes to take effect in the modem. (**Private LAN** is the default for **DHCP Server.**)

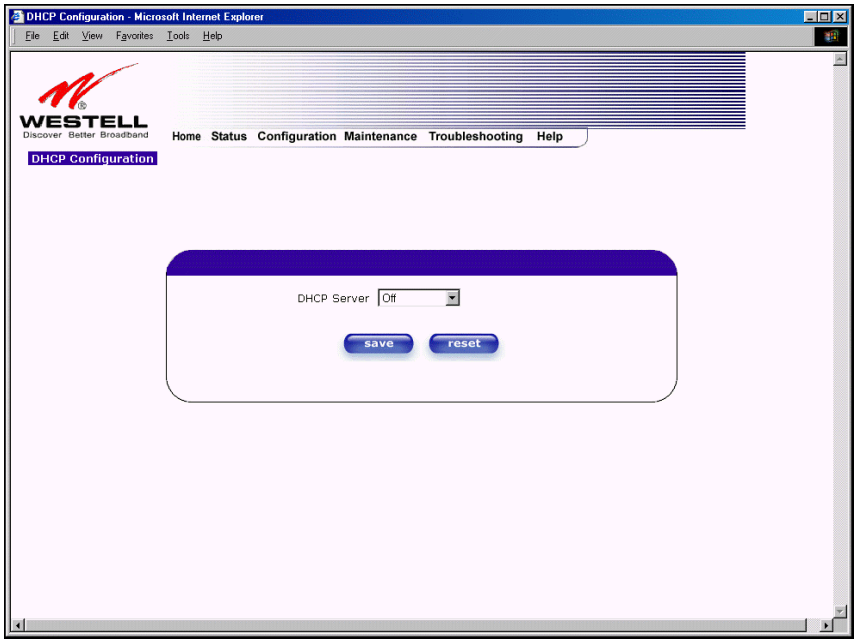


If you clicked **save**, in the preceding **DHCP Configuration** screen**,** the following pop-up screen will appear. Click on **OK** to continue.

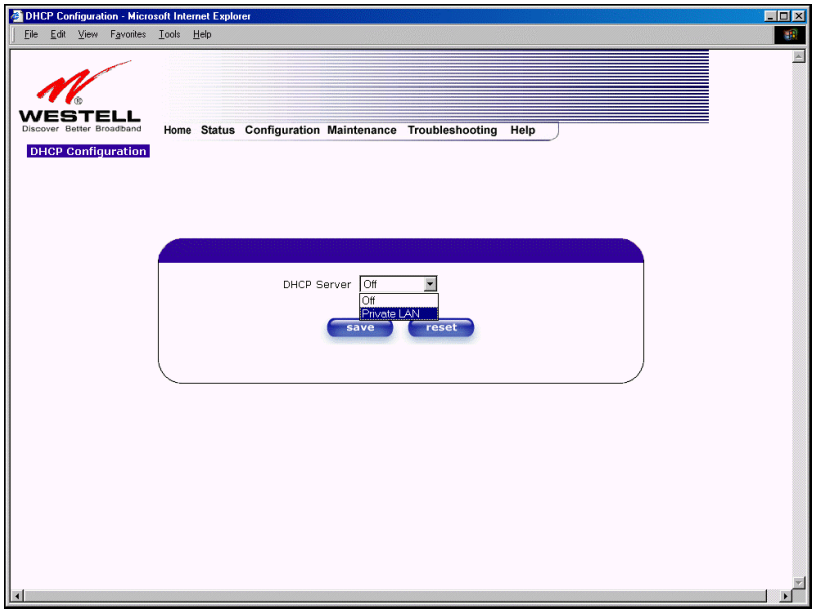
IMPORTANT: After you disable the DHCP server, reboot your PC to allow the changes to take effect.

13.5.4 Enabling the DHCP Server

To enable the DHCP Server (if it has previously been disabled), select **Advanced LAN > DHCP** from the **Configuration** menu. The following screen will be displayed.

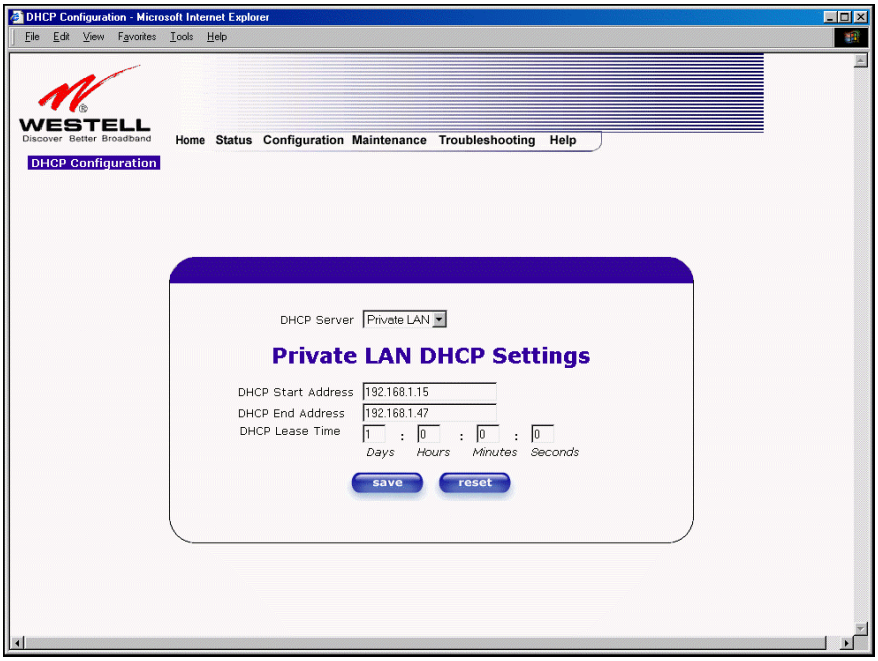


Next, select **Private LAN** from the **DHCP Server** drop-down menu.



If you selected **Private LAN** from the drop-down menu, the following screen will be displayed automatically. Now click **save** to save the settings. If you click **reset**, the screen will refresh and the previously saved settings will remain active.

IMPORTANT: Whenever you change the DHCP Server settings, the screen will display the changes; however, you must click **save** to allow the changes to take effect in the modem. (**Private LAN** is the default for **DHCP Server.**)



If you clicked **save**, the following pop-up screen will be displayed. Click **OK** to continue.

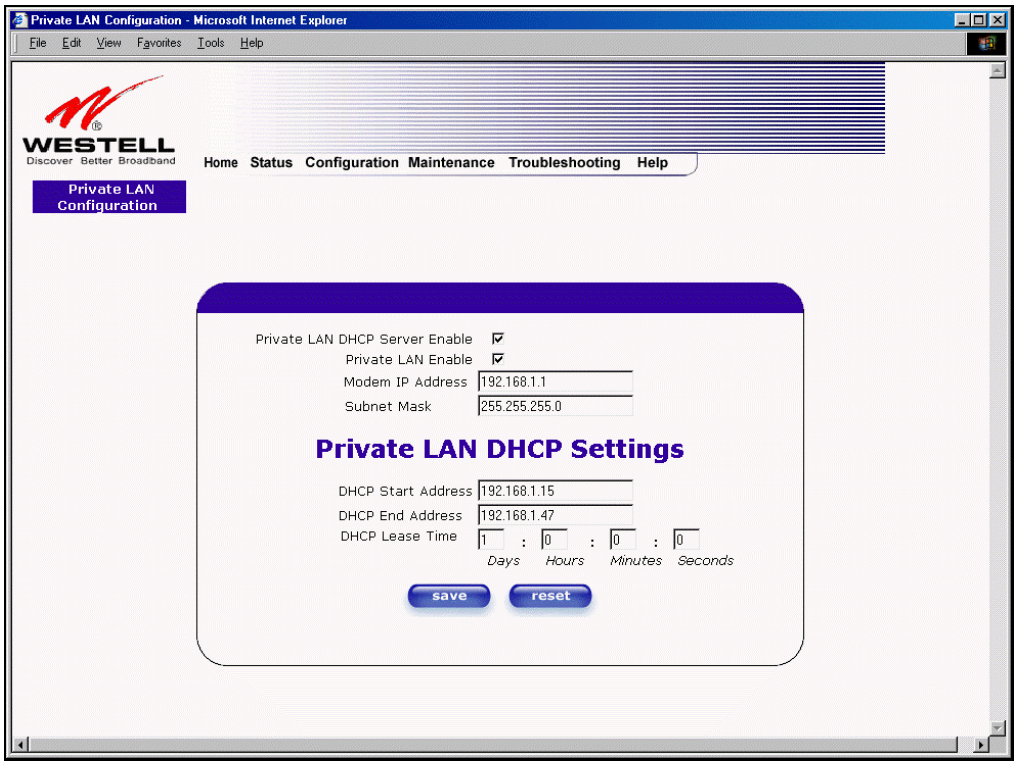
IMPORTANT: After you enable the DHCP server, reboot your PC to allow the changes to take effect.

13.5.5 Private LAN Configuration – Configuring NAT

The following screen will be displayed if you select **Advanced LAN > Private LAN** from the **Configuration** menu. Private LAN allows you to set up a network behind VersaLink.

If you change the settings in this screen, click **save**. If you click **reset**, the screen will refresh and the previously saved settings will remain active.

IMPORTANT: Whenever you change the Private LAN settings, the screen will display the changes; however, you must click **save** to allow the changes to take effect in the modem. (**Private LAN** is the default setting for VersaLink.)


Private LAN Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Private LAN Configuration
Private LAN DHCP Server Enable
Private LAN Enable
Modem IP Address 192.168.1.1
Subnet Mask 255.255.255.0
Private LAN DHCP Settings
DHCP Start Address 192.168.1.15
DHCP End Address 192.168.1.47
DHCP Lease Time 1 : 0 : 0 : 0
Days Hours Minutes Seconds
save
reset

If you made changes and clicked on **save,** the following pop-up screen will be displayed. Click **OK** to continue. If you click **Cancel**, your new settings will not take effect.

Private LAN DHCP Server Enable	Default = CHECKED If this box is CHECKED, it enables DHCP addresses to be served from the Private LAN pool.
Private LAN Enable	Default = CHECKED If this box is CHECKED, it enables the addresses from the Private LAN to use the NAT interface.
Modem IP Address	Displays VersaLink's IP address
Subnet Mask	Displays the Subnet Mask, which determines what portion of an IP address is controlled by the network and which portion is controlled by the host.
DHCP Start Address	Displays the first IP address that the DHCP server will provide.
DHCP End Address	Displays the last IP address that the DHCP server will provide.
DHCP Lease Time	Displays the amount of time the provided addresses will be valid, after which the DHCP client will usually re-submit a request.
Note: The DHCP Lease Time value must be greater than 10 seconds. The default = 01:00:00:00. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.	

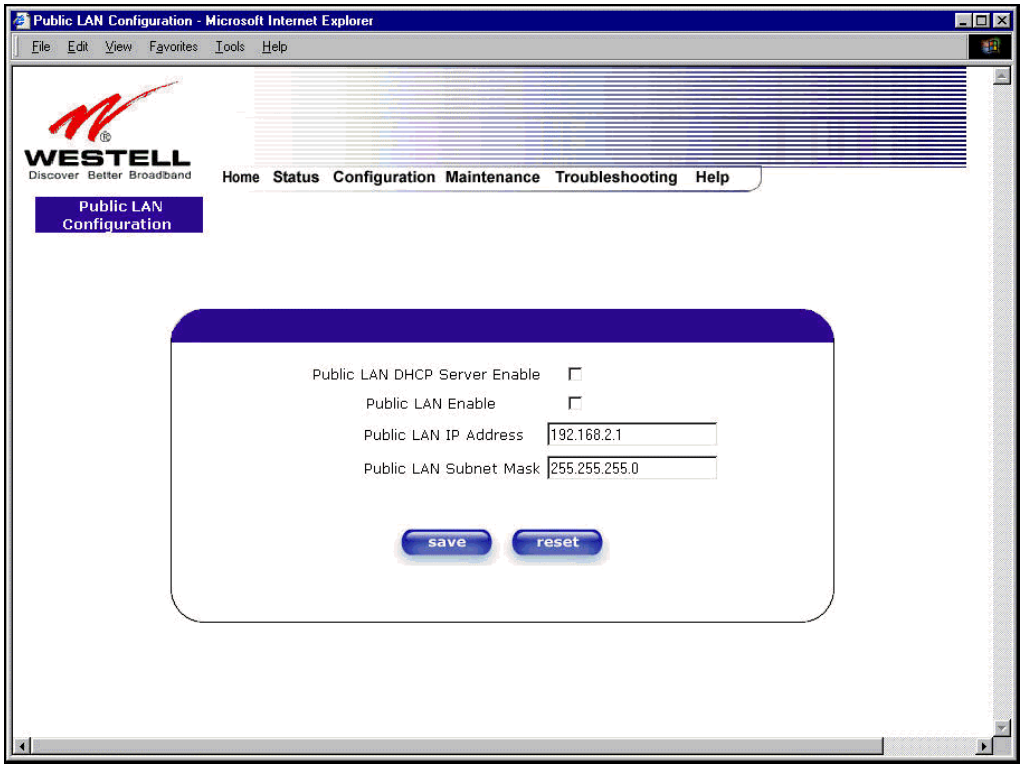
If the settings you have entered in the **Private LAN Configuration** screen are incorrect, the following warning messages may be displayed in pop-up screens. If this occurs, check the settings in the **Private LAN Configuration** screen.

Warning Message	Check Private LAN DHCP Settings
Start Address is not part of the Subnet	Check the value in the DHCP Start Address field
End Address is not part of the Subnet	Check the value in the DHCP End Address field
End Address is below the Start Address	Check the value in the DHCP End Address field
Lease time must be greater than 10 seconds	Check the values in the DHCP Lease Time fields
Seconds must be between 0 and 59	Check the **Seconds** value in the DHCP Lease Time field
Minutes must be between 0 and 59	Check the **Minutes** value in the DHCP Lease Time field
Hours must be between 0 and 23	Check the **Hours** value in the DHCP Lease Time field

13.5.6 Public LAN Configuration – Multiple IP Address PassThrough

The following screen will be displayed if you select **Advanced LAN > Public LAN** from the **Configuration** menu. Click the **Public LAN DHCP Server Enable** box (a check mark will appear in the box).

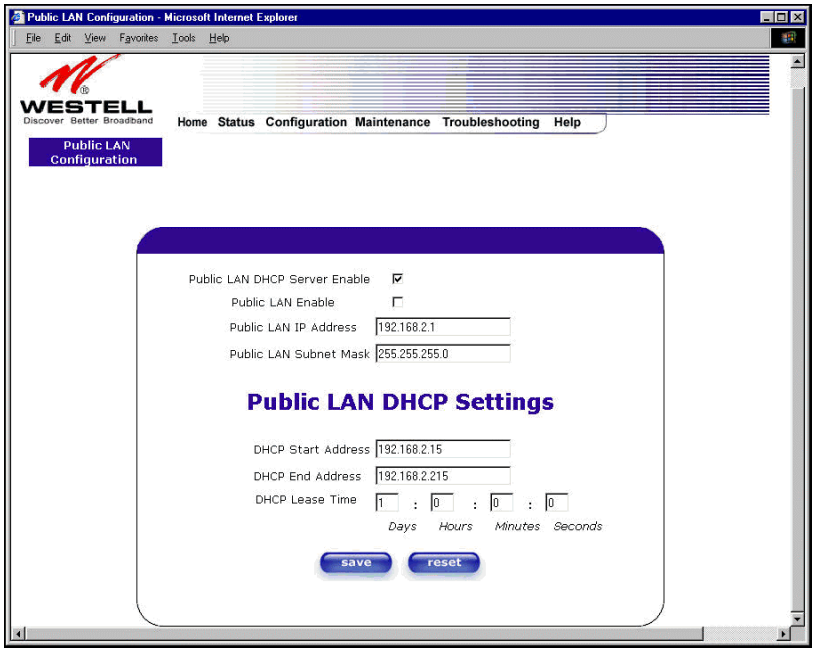
NOTE: The Public LAN feature, if available from your service provider, allows VersaLink to use LAN IP addresses that are accessible from the WAN. Public LAN allows your computer to have global address ability. To utilize the Public LAN feature on VersaLink, your ISP must support Public LAN and Static IP. Contact your ISP for details.



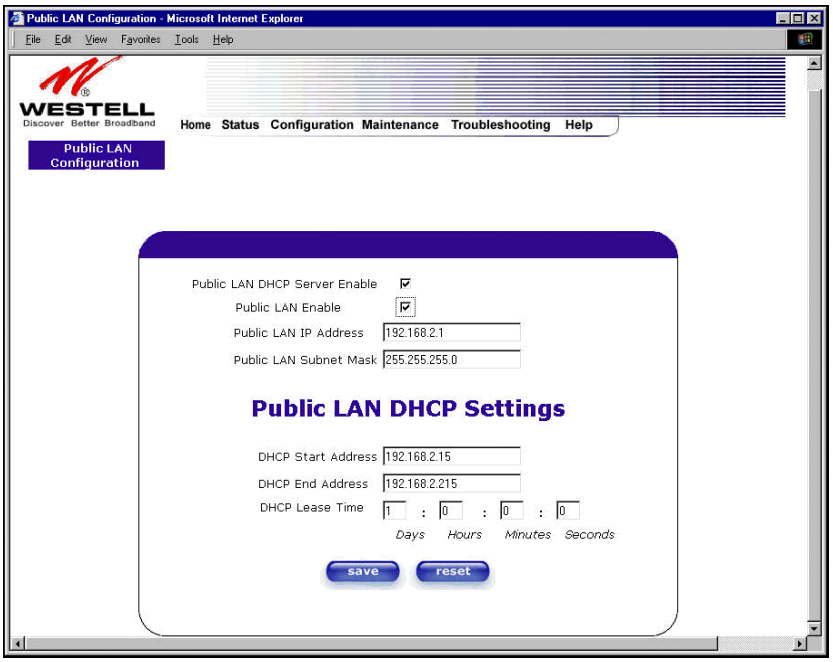
Public LAN DHCP Server Enable	Default = NOT CHECKED If this box is CHECKED, it enables DHCP addresses to be served from the Public LAN pool.
Public LAN Enable	Default = NOT CHECKED If this box is CHECKED, it enables the addresses from the Public LAN to bypass the NAT interface.
Public LAN IP Address	Provides a Public IP Address if the service provider does not automatically provide one.
Public LAN Subnet Mask	Provides a Public Subnet Mask if the service provider does not automatically provide one.

If you clicked in the **Public LAN DHCP Server Enable** box, the following screen will be displayed automatically. Click the **Public LAN Enable** box (a check mark will appear in the box).

NOTE: By enabling the Public LAN DHCP Server, you automatically disable VersaLink's the Private LAN DHCP Server. (**Private LAN DHCP** is the default setting for VersaLink.)


Public LAN Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Public LAN Configuration
Public LAN DHCP Server Enable
Public LAN Enable
Public LAN IP Address 192.168.2.1
Public LAN Subnet Mask 255.255.255.0
Public LAN DHCP Settings
DHCP Start Address 192.168.2.15
DHCP End Address 192.168.2.215
DHCP Lease Time 1 : 0 : 0 : 0
Days Hours Minutes Seconds
save reset

If you clicked the **Public LAN Enable** box, the following screen will be displayed automatically. The check marks indicates that **Public LAN Enable** is selected. Now click **save** to allow the settings to take effect.


Public LAN Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Public LAN Configuration
Public LAN DHCP Server Enable
Public LAN Enable
Public LAN IP Address 192.168.2.1
Public LAN Subnet Mask 255.255.255.0
Public LAN DHCP Settings
DHCP Start Address 192.168.2.15
DHCP End Address 192.168.2.215
DHCP Lease Time 1 : 0 : 0 : 0
Days Hours Minutes Seconds
save reset

If you selected **Public LAN Enable,** or if you made other changes in the **Public LAN Configuration** screen and clicked **save**, the following pop-up screen will be displayed. Click **OK** to save the new settings. If you click **Cancel**, your new settings will not take effect.

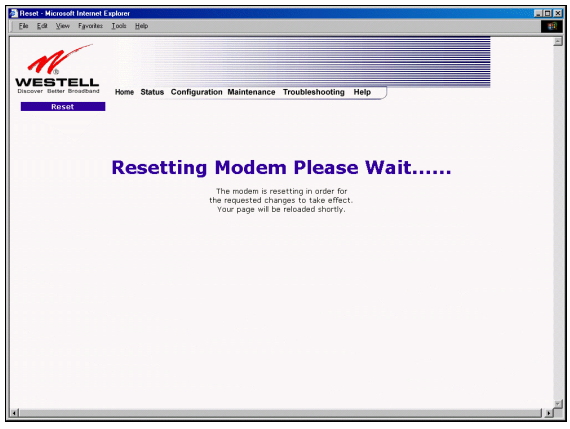
If the settings you have entered in the **Public LAN Configuration** screen are incorrect, the following warning messages may be appear in pop-up screens. If this occurs, check the **Public LAN Configuration** settings.

Warning Message	Check Public LAN DHCP Settings
Start Address is not part of the Subnet	Check the value in the DHCP Start Address field
End Address is not part of the Subnet	Check the value in the DHCP End Address field
End Address is below the Start Address	Check the value in the DHCP End Address field
Lease time must be greater than 10 seconds	Check the values in the DHCP Lease Time fields
Seconds must be between 0 and 59	Check the **Seconds** field at DHCP Lease Time
Minutes must be between 0 and 59	Check the **Minutes** field at DHCP Lease Time
Hours must be between 0 and 23	Check the **Hours** field at DHCP Lease Time
Note: The DHCP Lease Time value must be greater than 10 seconds. The default = 01:00:00:00. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.	

If you clicked **OK** in the **Load new Public LAN configuration?** screen, the following pop-up screen will be displayed. Click **OK** to continue.

Microsoft Internet Explorer
The modem must be reset in order for the new configuration to take affect.
Do you wish to reset now?
OK
Cancel

If you clicked **OK** in the preceding screen**,** the following screen will be displayed. VersaLink will be reset and the new configuration will take effect.

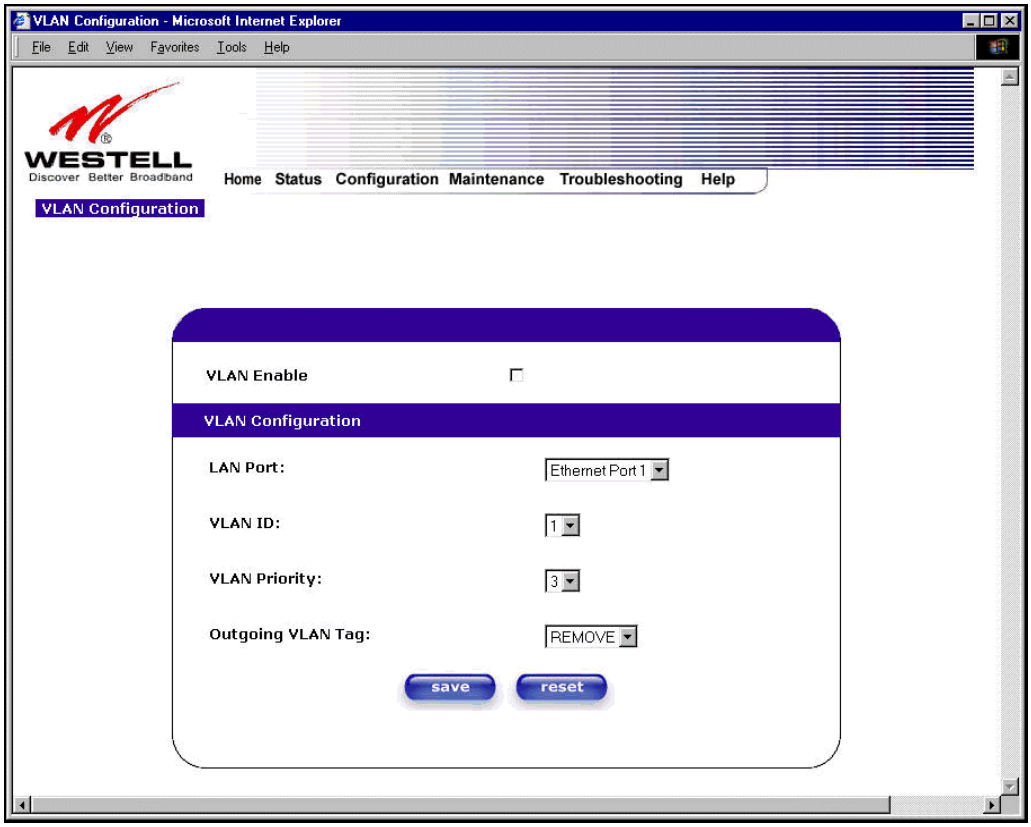

WESTELL
Home Status Configuration Maintenance Troubleshooting Help
Reset
Resetting Modem Please Wait.....
The modem is resetting in order for the requested changes to take effect.
Your page will be reloaded shortly.

After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP.** (If necessary, click the **connect** button to establish a PPP session).

13.5.7 VLAN

The following screen will be displayed if you select **Advanced LAN > VLAN** from the **Configuration** menu.

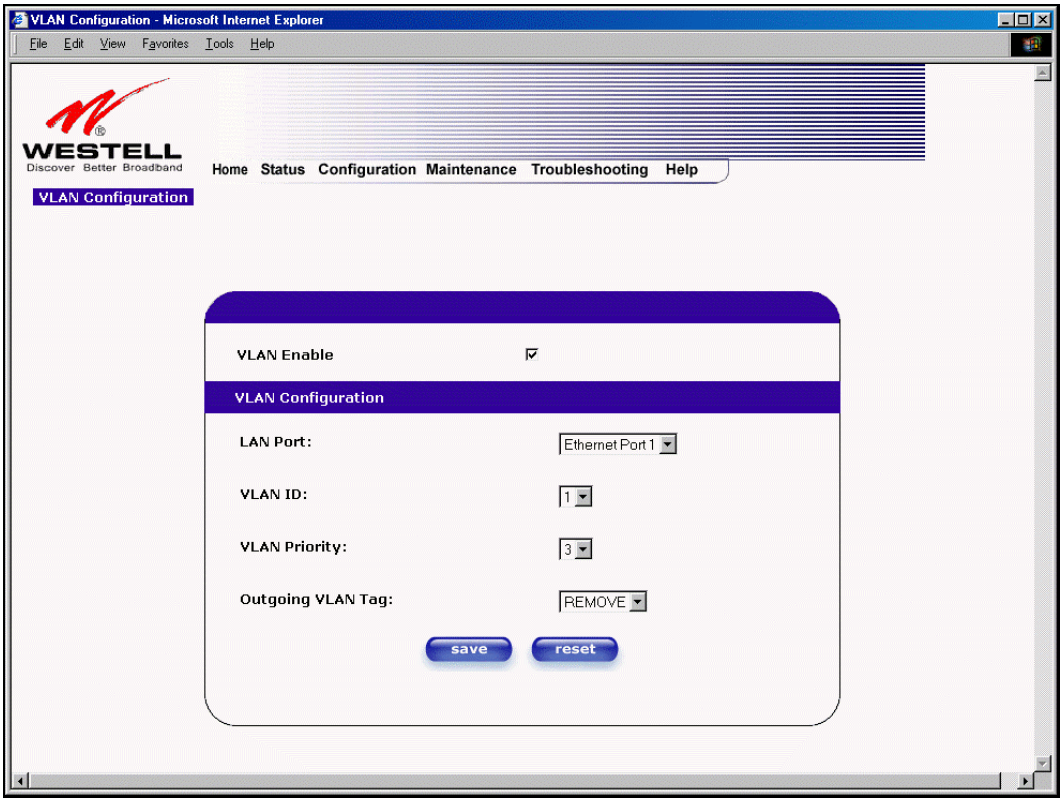
NOTE: If VersaLink is configured using **ETHERNET PORT 1**, the following screen will not be available.



VLAN Enable	Factory Default = DISABLED If this box is check, VLAN will be Enabled. This will allow VLAN tagging to occur according to the data port's configuration.
LAN Port	This allows you to select the LAN port that you wish to configure. Possible responses are: Ethernet Port 1 Ethernet Port 2 Ethernet Port 3 Ethernet Port 4 WLAN Port
VLAN ID	This allows you to assign a VLAN ID to the port. Possible responses are: 1 through 8
VLAN Priority	This allows you to set the VLAN priority for the port. Possible responses are: 0 through 7
Outgoing VLAN Tag	This allows you to keep or remove the VLAN tag on the port when data is outgoing.

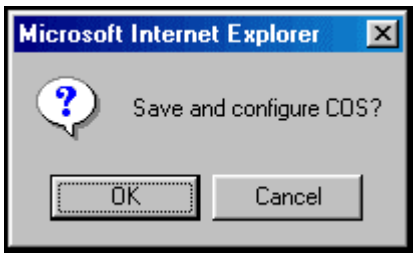
To enable VLAN, click the **VLAN Enable** box (a check mark will appear in the box). Next, select the desired settings from the drop-down menus, and then click **save** to continue.

NOTE: For VLAN to function properly, the VLAN ID must be set to a value other than '1' in the **VLAN Configuration** screen and in the **VC 1 Configuration** screen when the you are using the Bridge (VLAN Bridge) protocol. See Advanced WAN section for configuring VC's (refer to section 13.6.3.3).



NOTE: If you change the values in the **VLAN Configuration** screen, you must click **save** to save the settings. If you click **reset**, the screen will refresh and display the previously saved settings for the LAN Port you have selected.

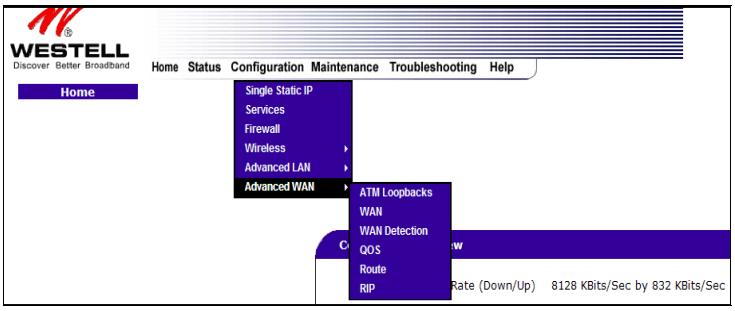
If you click **save**, the following pop-up screen will be displayed. Click **OK** in the pop-up screen to allow the new settings to take effect.



13.6 Advanced WAN

This section explains the configurable features of VersaLink that are available if you select **Advanced WAN** from the **Configuration** menu.

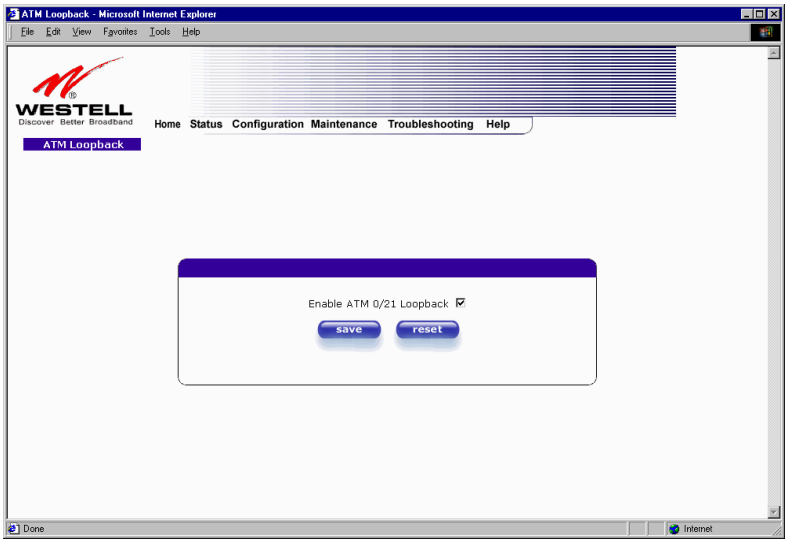
NOTE: If VersaLink is configured for **ETHERNET PORT 1**, **QOS** will not be displayed. You must configure VersaLink for **DSLATM PORT** to access **QOS** in the **Advanced WAN** drop-down menu. Refer to section 13.6.2.2 for details.



13.6.1 ATM Loopbacks

If you select **Advanced WAN > ATM Loopbacks** from the **Configuration** menu, the following screen will be displayed.

NOTE: When the **Enable ATM 0/21** box is checked, this feature is enabled. If the box does not display a check mark, this feature is disabled. If you change the setting in this screen, you must click **save,** and then click **OK** in the pop-up screen. **Westell recommends that you do not change this setting.**



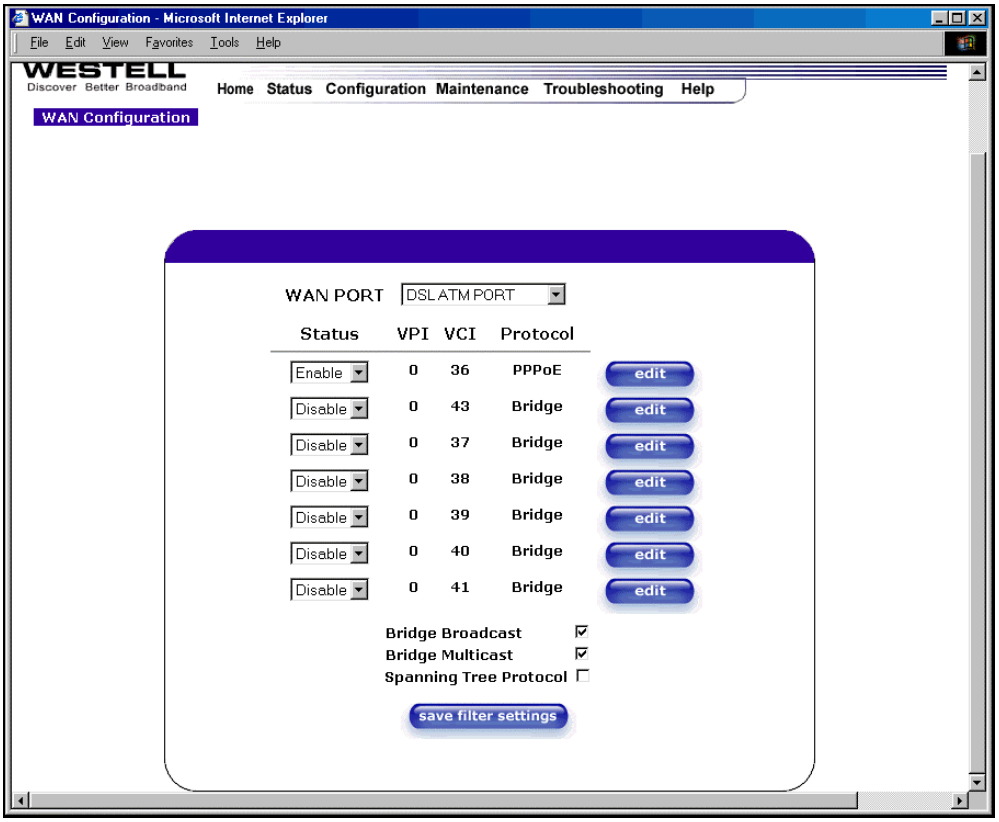
Enable ATM 0/21 Loopback:	Factory Default = ENABLED This option enables the 0/21 loopback , which is used by your ISP. Note: Westell recommends that you do not that you change this setting.

13.6.2 WAN Configuration

The following screen will be displayed if you select **Advanced WAN > WAN** from the Configuration menu.

If you change the **Bridge Broadcast, Bridge Multicast,** or **Spanning Tree Protocol** configurations in this screen, click the **save filter settings** button to allow these changes to take effect. If you change any of the **Status** configurations, a pop-up screen will prompt you to reset the Gateway. After the Gateway has been reset, the **Status** configurations will take effect. The **edit** button allows you to change the VC configuration settings of the Gateway. Details on the **edit** button are explained later in section 13.6.3, "Editing the WAN Configuration."

NOTE: The actual information displayed in this screen may vary, depending on the network connection established.


WAN Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
WAN Configuration
WAN PORT DSL ATM PORT
Status VPI VCI Protocol
Enable 0 36 PPPoE edit
Disable 0 43 Bridge edit
Disable 0 37 Bridge edit
Disable 0 38 Bridge edit
Disable 0 39 Bridge edit
Disable 0 40 Bridge edit
Disable 0 41 Bridge edit
Bridge Broadcast
Bridge Multicast
Spanning Tree Protocol
save filter settings

WAN PORT	Factory Default = DSLATM PORT Possible Responses: DSLATM PORT ETHERNET PORT 1
Status	Allows you to enable or disable your VC (Virtual Connection)
VPI	Displays the VPI (Virtual Path Indicator) value for a particular VC, which is defined by your Service Provider.
VCI	Displays the VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your Service Provider.
Protocol NOTE: The configuration specified by your Service Provider will determine which Protocols are available to you.	Displays the Protocol for each VC, which is specified by your Service Provider. PPPoA = Point to Point Protocol over ATM (Asynchronous Transfer Mode) PPPoE = Point to Point Protocol over Ethernet Bridge = Bridge Protocol Classical IPoA = Internet Protocol over ATM (Asynchronous Transfer Mode). This is an ATM encapsulation of the IP protocol.
Bridge Broadcast	Factory Default = CHECKED When this setting is CHECKED, VersaLink will allow Broadcast IP packets to/from the WAN. When this setting is NOT CHECKED, VersaLink will block Broadcast IP packets to/from the WAN. This setting is only valid if one of the Virtual Channels is configured for Bridge mode.
Bridge Multicast	Factory Default = CHECKED When this setting is CHECKED, VersaLink will allow Multicast IP packets to/from the WAN. When this setting is NOT CHECKED, VersaLink will block Multicast IP packets to/from the WAN. This setting is only valid if one of the Virtual Channels is configured for Bridge mode.
Spanning Tree Protocol	Factory Default = DISABLED Spanning Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For Ethernet network to function properly, only one active path can exist between two stations. When ENABLED, two bridges are used to interconnect the same two computer network segments. Spanning Tree Protocol will allow the bridges to exchange information so that only one of them will handle a given message that is being sent between two computers within the network. NOTE: Spanning Tree can't be enabled if VLAN is enabled.

13.6.2.1 Disabling DSLATM PORT – Enabling ETHERNET PORT 1

To configure VersaLink for uplink mode, select **ETHERNET PORT 1** from the **WAN PORT** drop-down menu. By selecting **ETHERNET PORT 1**, you will disable VersaLink's DSL transceiver. This will disable the DSL port on the rear of the Gateway and enable the **ETHERNET1** port for use as the WAN Ethernet uplink interface.

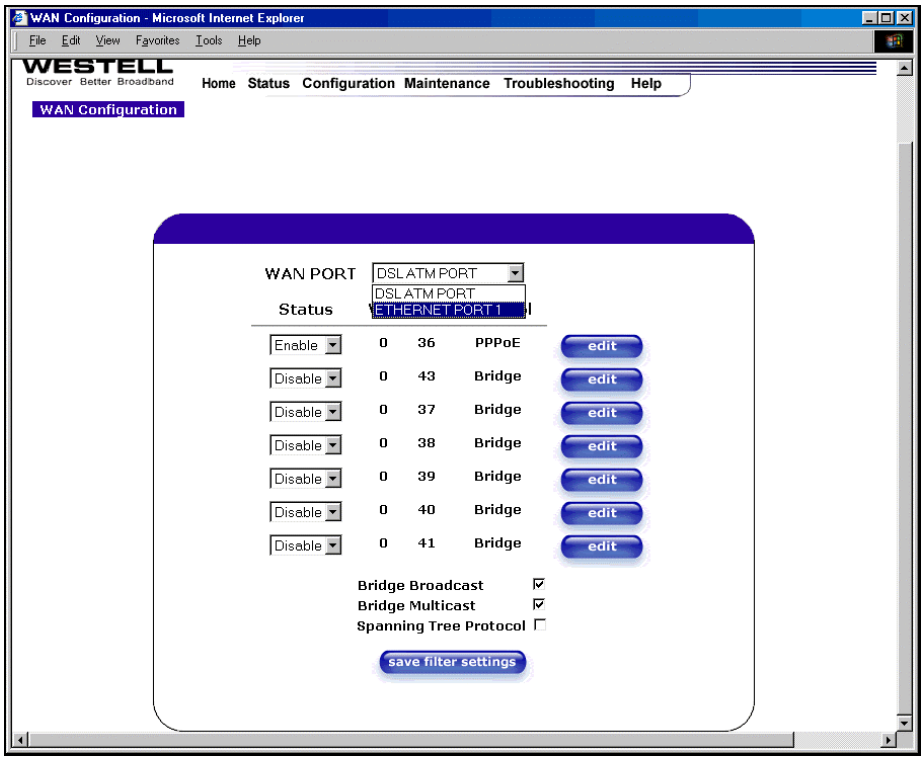
NOTE:

1) If you select **ETHERNET PORT1,** only ports E2, E3, and E4 on the rear of the Gateway can be used for Ethernet LAN connection. ETHERNET1 will become the uplink port.

2) If you select **DSLATM PORT,** you can use all four ports (ETHERNET1, E2, E3, and E4) on the rear of the Gateway for Ethernet LAN connection.

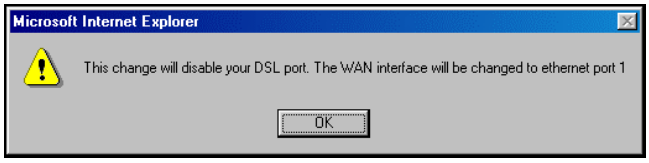
3) The uplink feature is optional, and when uplink is disabled, the Gateway will use DSL and wireless only.

4) All menu options are displayed when the Gateway is configured **DSLATM PORT.** However, some menu options may not be available when the Gateway is configured for **ETHERNET PORT 1.**

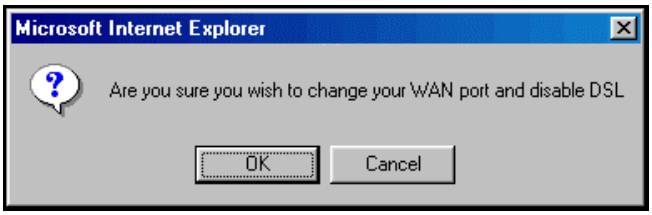


NOTE: If you experience any problems, please reset VersaLink via the external hardware reset button or via the procedure defined under the **Maintenance** menu in section 15.1. (Factory defaults become current configuration.)

If you select **ETHERNET PORT 1** from the **WAN Port** drop-down arrow, the following screen will be displayed. Click **OK.**


Microsoft Internet Explorer
This change will disable your DSL port. The WAN interface will be changed to ethernet port 1
OK

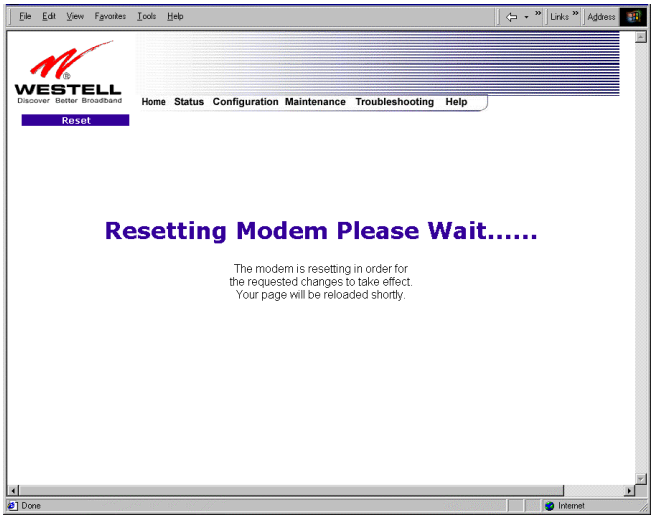
If you clicked **OK** in the preceding pop-up screen, the following screen will be displayed. Click on **OK.** If you click on **Cancel,** the change will not take effect.



If you clicked **OK** in the preceding pop-up screen, the following pop-up screen will appear. VersaLink must be reset to allow the new configuration to take effect. Click on **OK.**

Microsoft Internet Explorer
The modem must be reset in order for the new configuration to take affect.
Do you wish to reset now?
OK
Cancel

If you clicked **OK**, VersaLink will be reset and the new configuration will take effect.


WESTELL
Home Status Configuration Maintenance Troubleshooting Help
Reset
Resetting Modem Please Wait.....
The modem is resetting in order for
the requested changes to take effect.
Your page will be reloaded shortly.

After VersaLink has been reset, the **DSL** LED will be OFF. This is because the DSL transceiver has been disabled. However, the **Power, Ethernet**, and **Wireless** LEDs will remain lit.

13.6.2.2 Enabling DSLATM PORT – Disabling ETHERNET PORT 1

If **ETHERNET PORT 1** has previously been enabled and you want to disable it and enable **DSLATM PORT,** select **Advanced WAN > WAN** from the **Configuration** menu. The following screen will be displayed.

Next, select **DSLATM PORT** from the **WAN PORT** drop-down menu. By selecting **DSLATM PORT**, you will enable VersaLink's DSL transceiver. This will disable the WAN Ethernet uplink port and allow the WAN interface to use the DSL port.

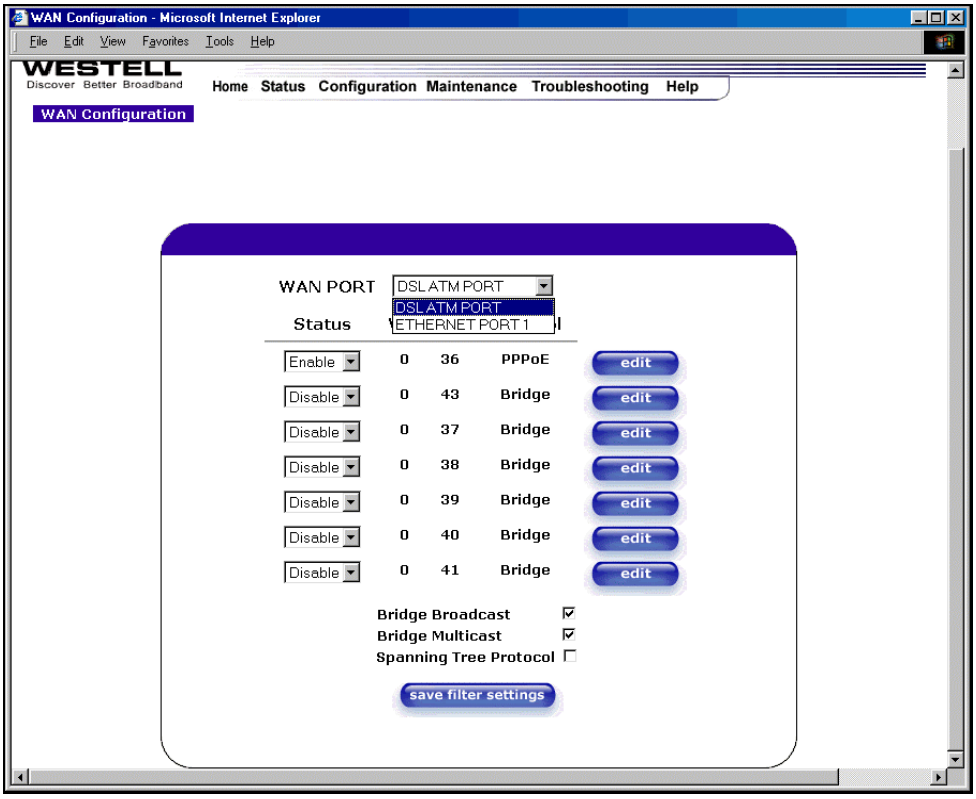
NOTE:

1) If you select **DSLATM PORT,** you can use all four ports (ETHERNET1, E2, E3, and E4) on the rear of the Gateway for Ethernet LAN connection.

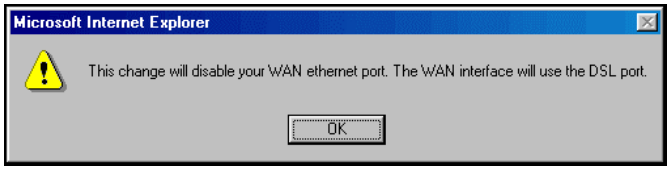
2) If you select **ETHERNET PORT1,** only ports E2, E3, and E4 on the rear of the Gateway can be used for Ethernet LAN connection. ETHERNET1 will become the uplink port.

3) The uplink feature is optional, and when uplink is disabled, the Gateway will use DSL and wireless only.

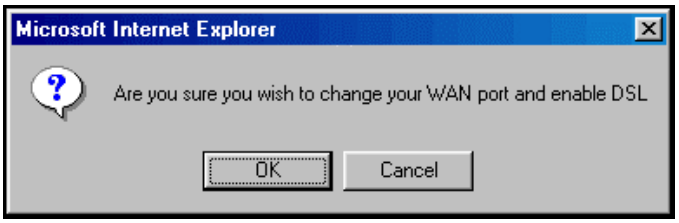
4) All menu options are displayed when the Gateway is configured **DSLATM PORT.** However, some menu options may not be available when the Gateway is configured for **ETHERNET PORT 1.**



If you select **DSLATM PORT** from the **WAN Port** drop-down menu, the following screen will be displayed. Click **OK.**



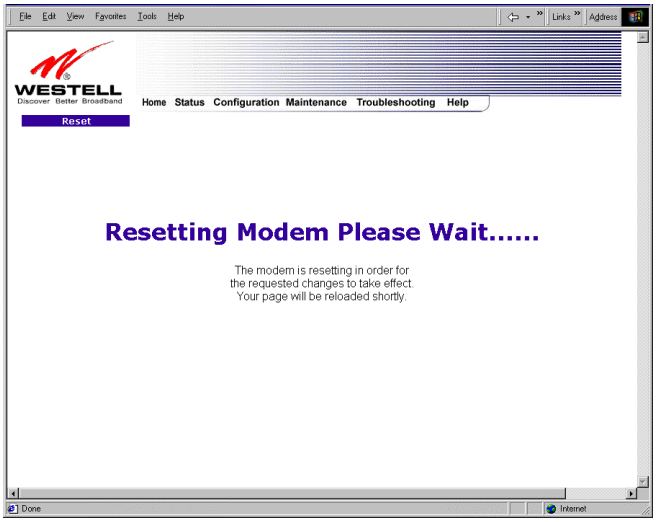
If you click **OK** in the preceding pop-up screen, the following screen will be displayed. Click **OK.** If you click **Cancel,** the change will not take effect.



If you clicked **OK** in the preceding pop-up screen, the following pop-up screen will be displayed. VersaLink must be reset to allow the new configuration to take effect. Click **OK.**

Microsoft Internet Explorer
The modem must be reset in order for the new configuration to take affect.
Do you wish to reset now?
OK
Cancel

If you clicked **OK,** VersaLink will be reset and the new configuration will take effect.

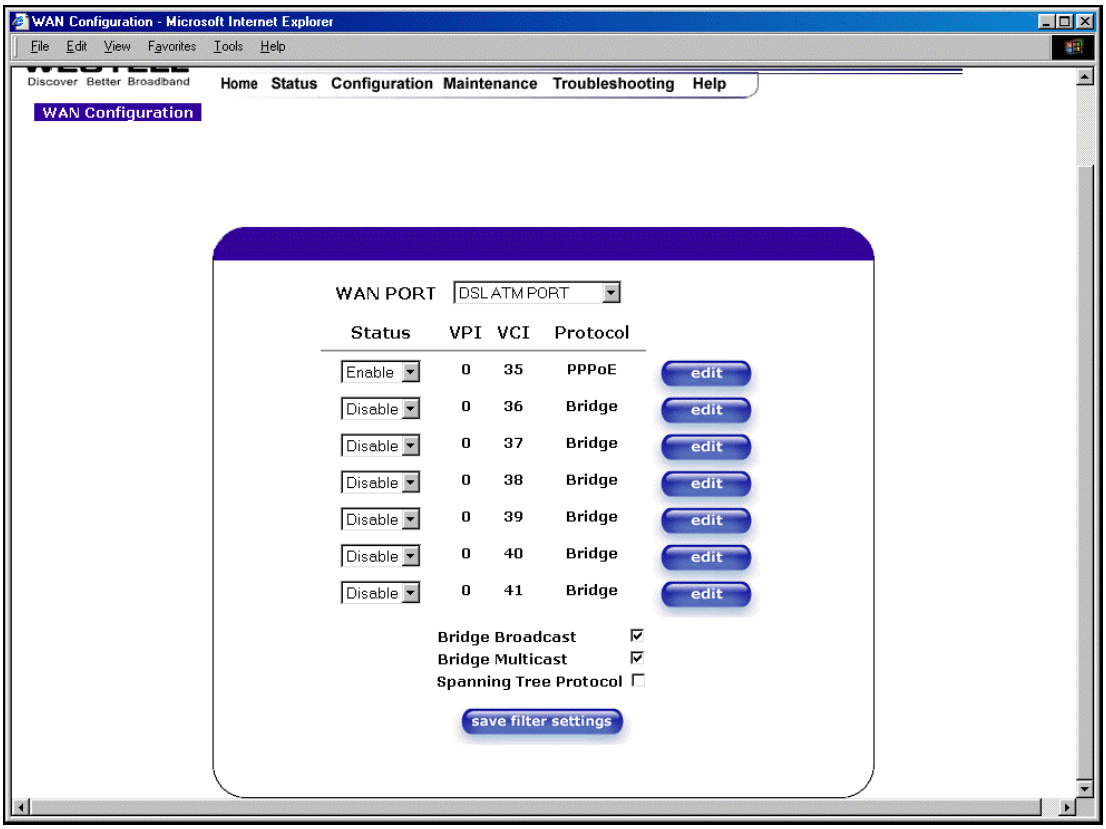


After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP.** (If necessary, click on the **connect** button to establish a PPP session).

13.6.3 Editing the WAN Configuration

To edit the WAN configuration of your VersaLink, select **Advanced WAN > WAN** from the **Configuration** menu. The following screen will be displayed. Next, click the **edit** button adjacent to any of the 'Enabled' protocols displayed in the **WAN Configuration** screen.

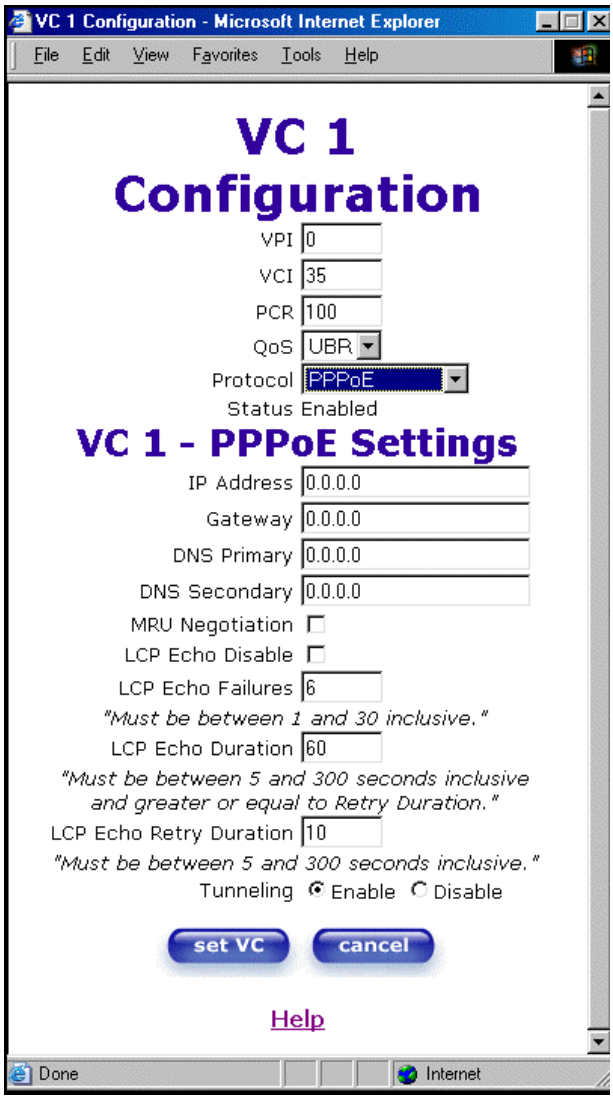
NOTE: The protocol status must display "Enable" to allow edits to its VC configuration.


WAN Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
WAN Configuration
WAN PORT DSL ATM PORT
Status VPI VCI Protocol
Enable 0 35 PPPoE edit
Disable 0 36 Bridge edit
Disable 0 37 Bridge edit
Disable 0 38 Bridge edit
Disable 0 39 Bridge edit
Disable 0 40 Bridge edit
Disable 0 41 Bridge edit
Bridge Broadcast
Bridge Multicast
Spanning Tree Protocol
save filter settings

If you clicked edit in the **WAN Configuration** screen, the following **VC 1 Configuration** screen will be displayed. The **VC 1 Configuration** screen allows you to edit your virtual connection (VC). A virtual connection identifies a connection through the service provider's ATM network to your ISP. Unlike physical hardware connections, virtual connections are defined by data.

If you change any settings in the **VC 1 Configuration** screen, click the **Set VC** button to save the settings.

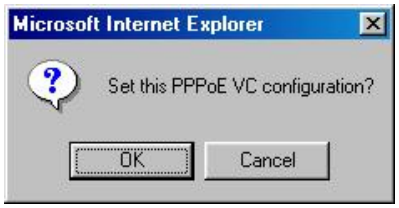
NOTE: If you experience any problems, please reset VersaLink via the external hardware reset button or via the procedure defined under the **Maintenance** menu in section 15.1. The actual information displayed in this screen may vary, depending on network connection established.



VC 1 Configuration	
VPI	This setting allows you to change your VPI (Virtual Path Indicator) value for a particular VC, which is defined by your Service Provider.
VCI	This setting allows you to change your VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your Service Provider.
PCR	Factory Default = 100% Peak Cell Rate (PCR)-The maximum rate at which cells can be transmitted across a virtual circuit, specified in cells per second and defined by the interval between the transmission of the last bit of one cell and the first bit of the next. This value is a percentage of the current data rate. 100 allows this VC to use 100% of the available bandwidth. 80 allows this VC to use 80% of the available bandwidth.
QoS	Quality of Service, which is determined by your Service Provider. Possible Responses: CBR = Constant Bit Rate UBR = Unspecified Bit Rate VBR = Variable Bit Rate
Protocol	The Protocol for each VC, which is specified by your Service Provider. Possible Responses: PPPoA = Point to Point Protocol over ATM (Asynchronous Transfer Mode) PPPoE = Point to Point Protocol over Ethernet Bridge = Bridge Protocol Classical IPoA = Internet Protocol over ATM (Asynchronous Transfer Mode). This is an ATM encapsulation of the IP protocol.
Status	The protocol status.
VC x PPPoE Settings	
IP Address	Displays the IP network address that your modem is on.
VersaLink	Displays VersaLink IP VersaLink address
DNS Primary	Provided by your Service Provider
DNS Secondary	Provided by your Service Provider
MRU Negotiation	Factory Default = DISABLED If ENABLED, the Maximum Received Unit (MRU) would enforce MRU negotiations. (NOTE: enable this option only at ISP's request.)
LCP Echo Disable	Factory Default = Enable If checked, this option will disable the modem LCP Echo transmissions.
LCP Echo Failures	Indicates number of continuous LCP echo non-responses received before the PPP session is terminated.
LCP Echo Retry Duration	The interval between LCP Echo transmissions with responses.
LCP Echo Retry Duration	The interval between LCP. Echo after no response.
Tunneling	Factory Default = ENABLE If ENABLED, this option allows PPP traffic to be bridged to the WAN. This feature allows you to use a PPPoE shim on the host computer to connect to your ISP, by bypassing VersaLink's capability to do this. NOTE: Tunneling is available using PPPoE protocol only.

NOTE: The values for IP Address, VersaLink, DNS Primary, and DNS Secondary are all "Override of the value obtained from the PPP connection," They default to "0.0.0.0," in which case the override is ignored. Westell recommends that you do not change the values unless your ISP instructs you to change them.

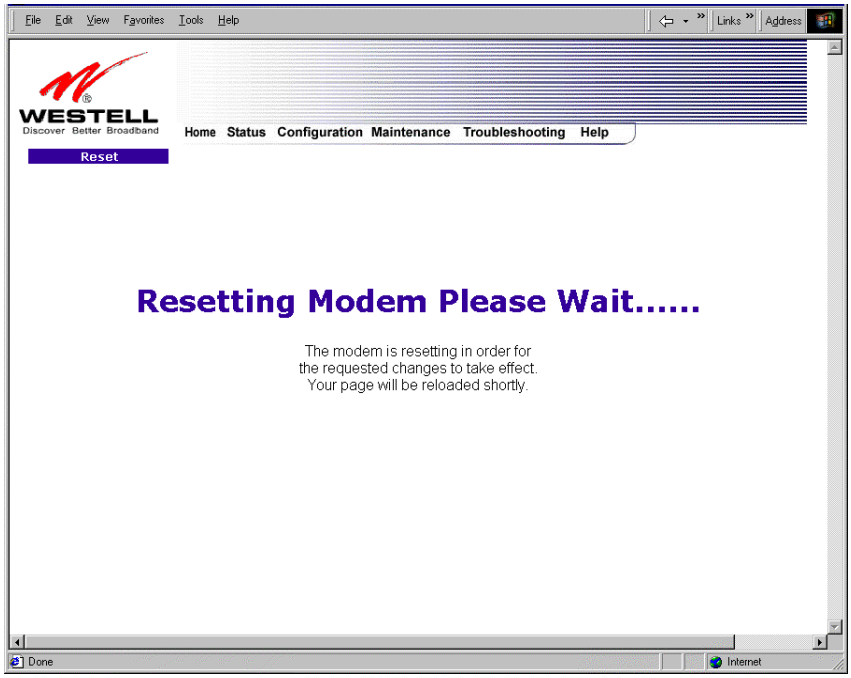
If you made changes and clicked the set VC button, the following pop-up screen will be displayed. Click OK when asked **Set this PPPoE VC configuration?** If you click on **cancel**, the new VC settings will not be saved.



If you clicked on **OK** in the preceding pop-up screen, the following pop-up screen will appear. Click **OK** to continue.

Microsoft Internet Explorer
The modem must be reset in order for the new configuration to take affect.
Do you wish to reset now?
OK
Cancel

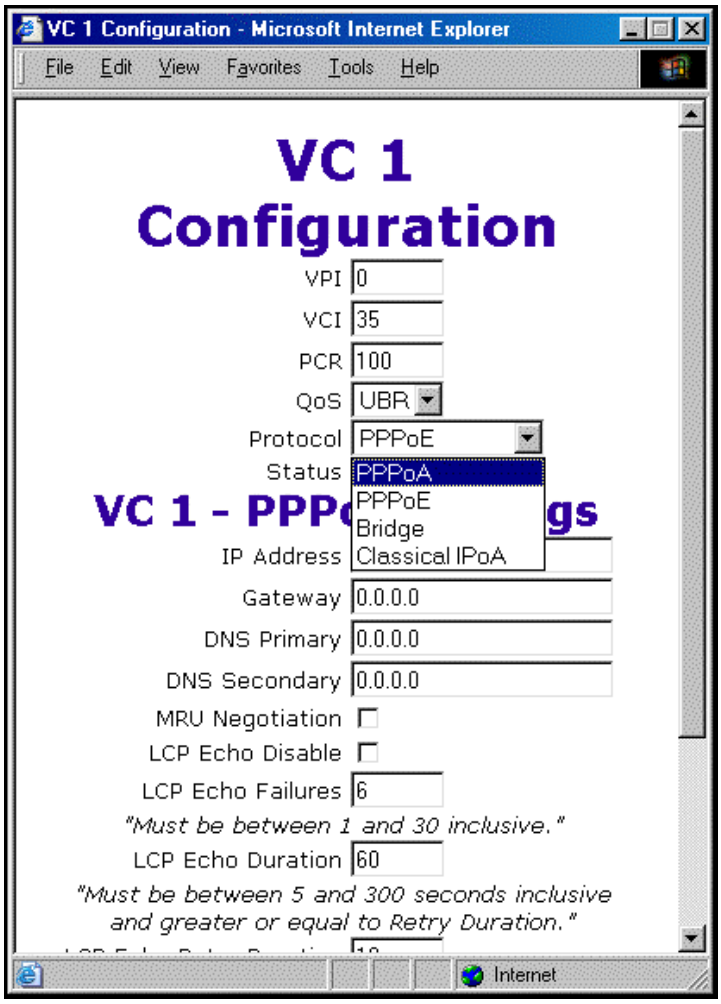
If you clicked **OK**, VersaLink will be reset and the new configuration will take effect.



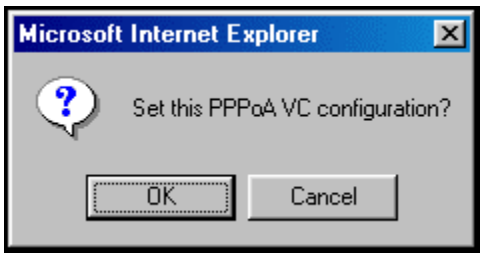
After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP.** (If necessary, click the **connect** button to establish a PPP session.)

13.6.3.1 Configuring VersaLink's Protocol Settings for PPPoA Mode

To configure VersaLink's protocol settings for PPPoA mode, select **PPPoA** from the **Protocol** drop-down menu. Next, click the **set VC** button to save the settings.

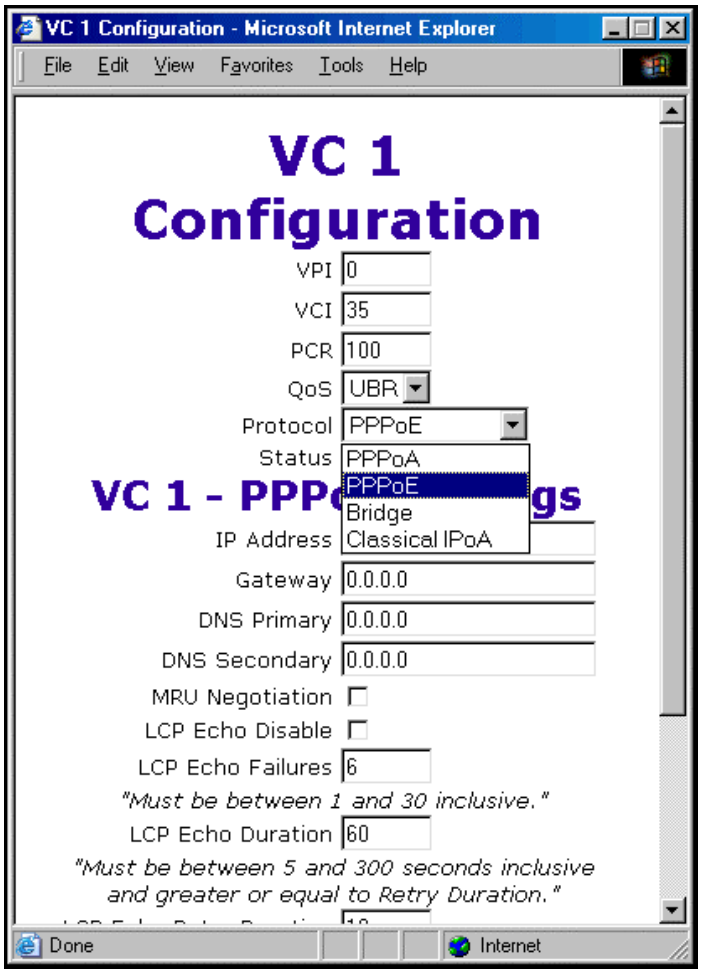


If you clicked the **set VC** button, the following pop-up screen will be displayed. Click on **OK** in the pop-up screen. If you click on **Cancel**, the new settings will not be saved. After you click on **OK,** follow the instructions to reset the Gateway, as previously discussed in section 13.6.3.

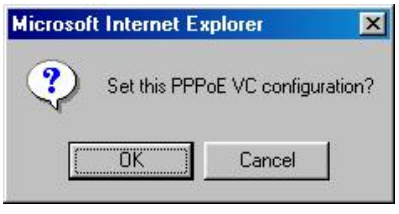


13.6.3.2 Configuring VersaLink's Protocol Settings for PPPoE Mode

To configure VersaLink's protocol settings for PPPoE mode, select **PPPoE** from the **Protocol** drop-down menu. Next, click the **set VC** button to save the settings.

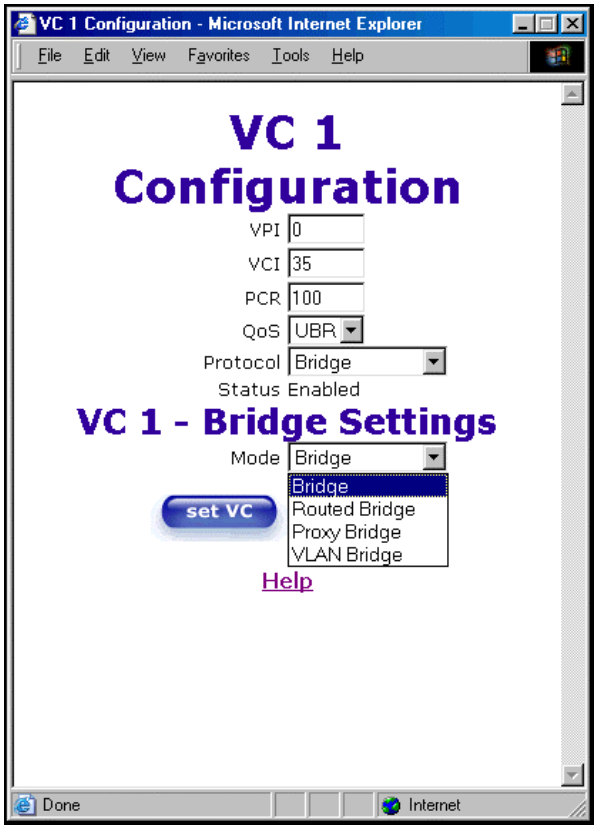


If you clicked the **set VC** button, the following pop-up screen will be displayed. Click on **OK** in the pop-up screen. If you click on **Cancel**, the new settings will not be saved. After you click on **OK,** follow the instructions to reset the Gateway, as previously discussed in section 13.6.3.



13.6.3.3 Configuring VersaLink's Protocol Settings for Bridge Mode

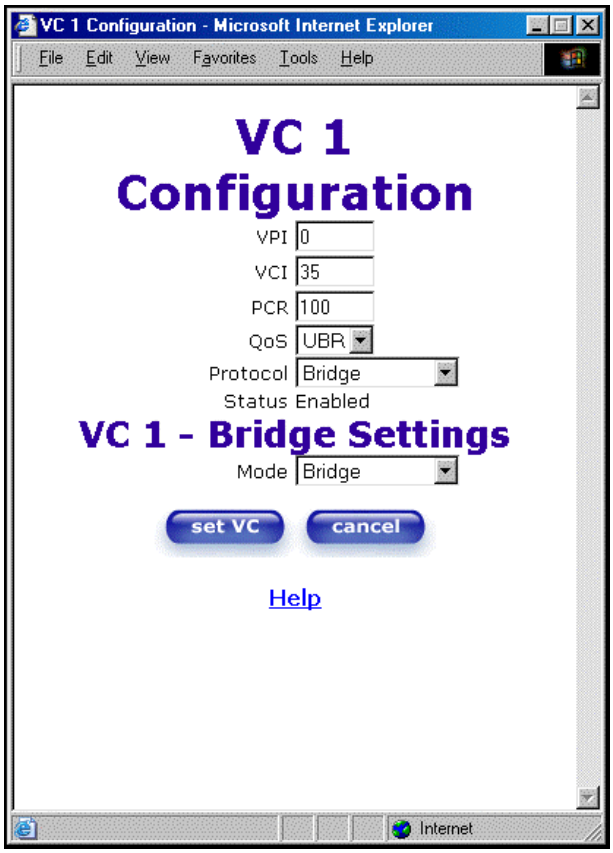
To configure VersaLink's protocol settings for Bridge mode, select **Bridge** from the **Protocol** drop-down menu. The following screen will be displayed. The **Mode** drop-down menu under **VC 1 –Bridge Settings** displays a list of options for your Bridge configuration. Select the desired option from the **Mode** drop-down menu. The following sections explain each mode.



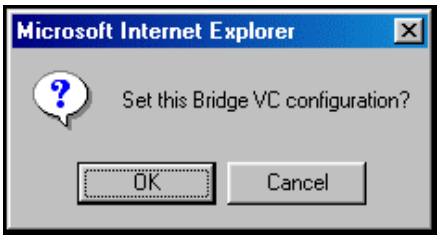
VC 1 Bridge Settings	
Mode	Bridge = A bridge is a layer 2 device that connects two segments of the same LAN that use the same protocol such as Ethernet. The modem does not have a WAN IP address in this mode. The client PC will typically get an IP address from a DHCP server in the network or the IP address can be assigned to the client PC statically.
	Routed Bridge = Routed Bridged Encapsulation (RBE) is the process by which a bridged segment is terminated on a routed interface. Specifically, VersaLink is routing on an IEEE 802.3 or Ethernet header carried over RFC 1483 bridged ATM. RBE was developed to address the known RFC1483 bridging issues, including broadcast storms and security. The modem will get a WAN IP address through DHCP or can be assigned statically. NAT will use the global address assigned to the modem.
	Proxy Bridge = Proxy Bridge is the process in which the modem acts as a proxy ARP agent for a local public subnet. The modem will be assigned an IP address from within that public subnet. The modem will direct all traffic to a VersaLink, which is configured statically. VersaLink address must not reside within VersaLink's assigned public subnet. All traffic will be sent via VersaLink's MAC address. The LAN may also have a private NAT'ed network. NAT will use the global address assigned to the modem.
	VLAN Bridge = Assigns VLAN tags to individual data ports on the modem.

13.6.3.3.1 Bridge Mode

If you selected **Bridge** mode under **VC 1- Bridge Settings,** the following screen will be displayed. Enter the appropriate values in the fields, and then click **set VC** to save the settings.

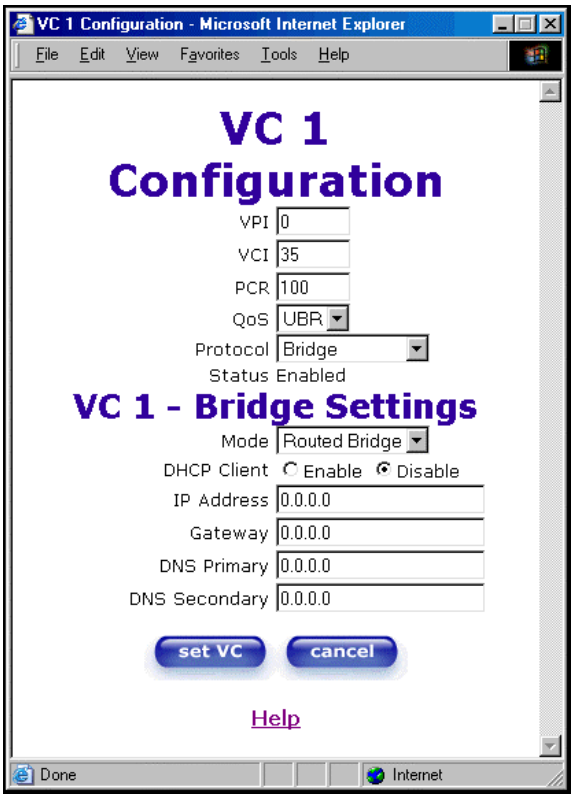


If you clicked the **set VC** button, the following pop-up screen will be displayed. Click on **OK** in the pop-up screen. If you click on **Cancel**, the new settings will not be saved. After you click on **OK,** follow the instructions to reset the Gateway, as previously discussed in section 13.6.3.



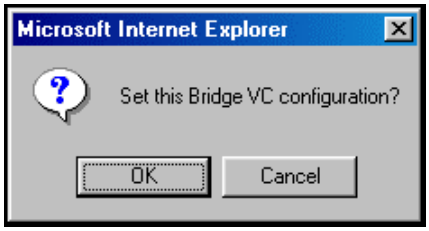
13.6.3.3.2 Routed Bridge Mode

If you selected **Routed Bridge** mode under **VC 1- Bridge Settings,** the following screen will be displayed. Enter the appropriate values in the fields, and then click **set VC** to save the settings.



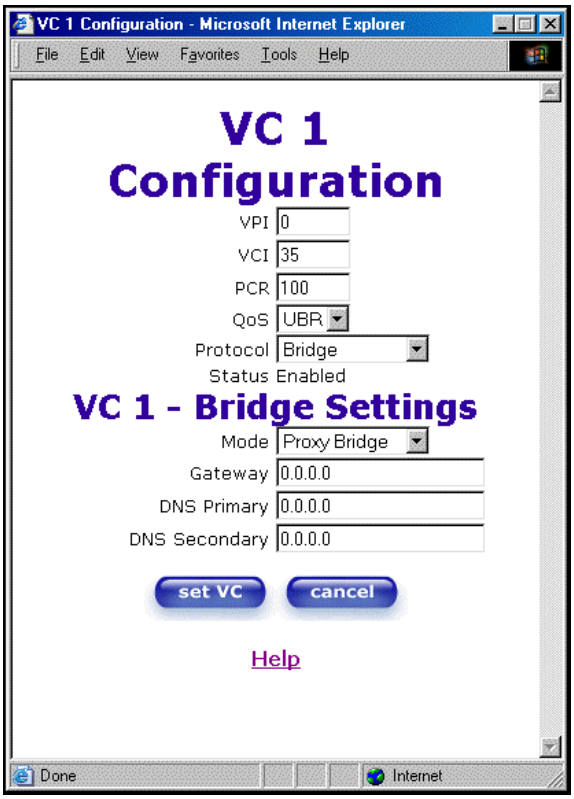
VC 1 - Bridge Settings (Routed Bridge)	
Mode	The Mode you have selected to use with Bridge protocol.
DHCP Client	Selecting a radio button allows you to either enable or disable the DHCP Client.
IP Address	Displays the IP network address that your modem is on.
Gateway	Displays the modem's IP gateway address.
DNS Primary	Provided by your ISP.
DNS Secondary	Provided by your ISP.

If you clicked the **set VC** button, the following pop-up screen will be displayed. Click on **OK** in the pop-up screen. If you click on **Cancel**, the new settings will not be saved. After you click on **OK,** follow the instructions to reset the Gateway, as previously discussed in section 13.6.3.



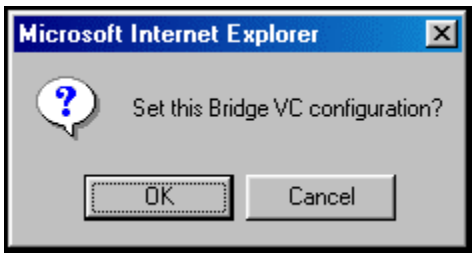
13.6.3.3.3 Proxy Bridge Mode

If you selected **Proxy Bridge** mode under **VC 1- Bridge Settings,** the following screen will be displayed. Enter the appropriate values in the fields, and then click **set VC** to save the settings.



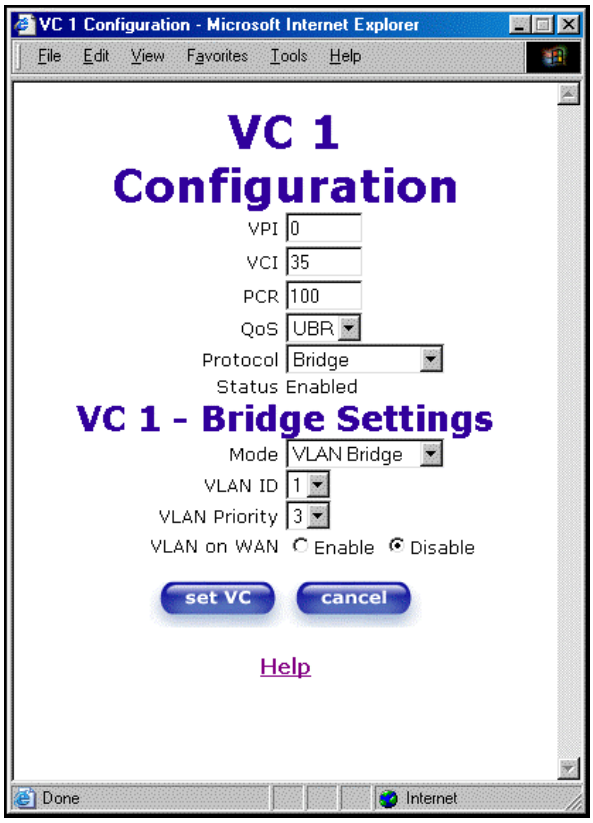
VC 1 - Bridge Settings (Proxy Bridge)	
Mode	The Mode you have selected to use with Bridge protocol.
Gateway	Displays the modem's IP address.
DNS Primary	Provided by your Service Provider.
DNS Secondary	Provided by your Service Provider.

If you clicked the **set VC** button, the following pop-up screen will be displayed. Click on **OK** in the pop-up screen. If you click on **Cancel**, the new settings will not be saved. After you click on **OK,** follow the instructions to reset the Gateway, as previously discussed in section 13.6.3.



13.6.3.3.4 VLAN Bridge Mode

If you selected **VLAN Bridge** mode under **VC 1- Bridge Settings,** the following screen will be displayed. Enter the appropriate values in the fields, and then click **set VC** to save the settings.

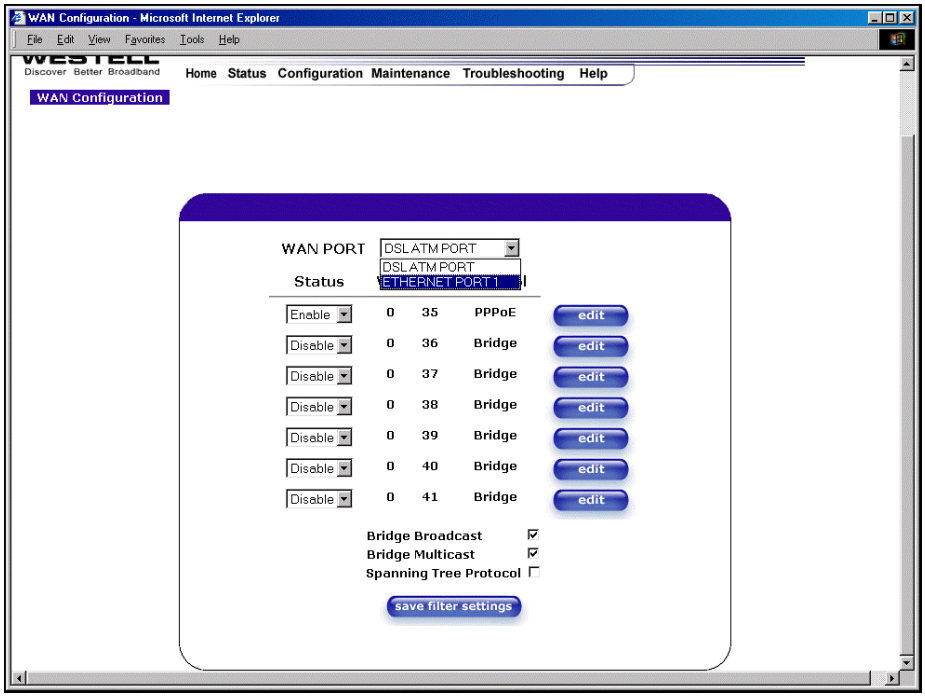


VC 1 - Bridge Settings (VLAN Bridge)	
Mode	The Mode you have selected to use with Bridge protocol. VLAN is used to assign VLAN tags to individual data ports on the modem.
VLAN ID	Assigns a VLAN ID to the port.
VLAN Priority	This will set the VLAN priority for the port.
VLAN on WAN	Factory Default = DISABLE Selecting Enable allows VLAN tagging to occur according to the data port's configuration.

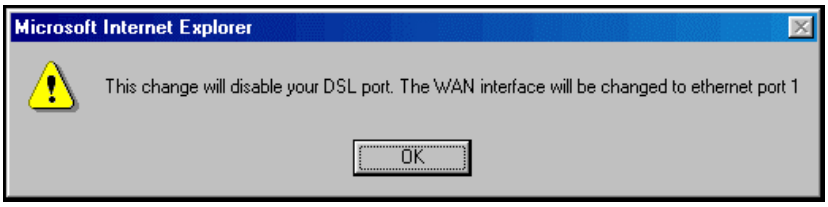
If you clicked the **set VC** button, the following pop-up screen will be displayed. Click on **OK** in the pop-up screen. If you click on **Cancel**, the new settings will not be saved. After you click on **OK,** follow the instructions to reset the Gateway, as previously discussed in section 13.6.3.

13.6.3.4 Configuring VC Protocol Settings for ETHERNET PORT 1

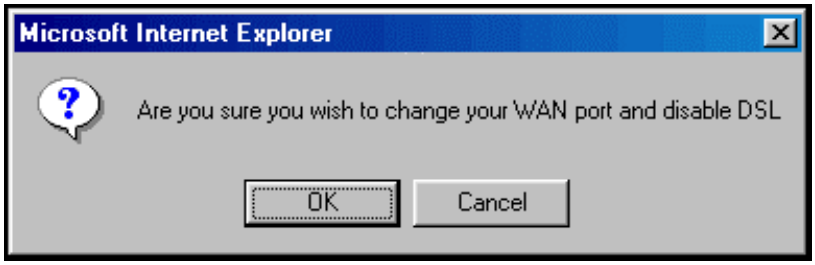
To configure VersaLink's VC settings to use the WAN Ethernet uplink port, select **ETHERNET PORT 1** at the **WAN Port** drop-down arrow.



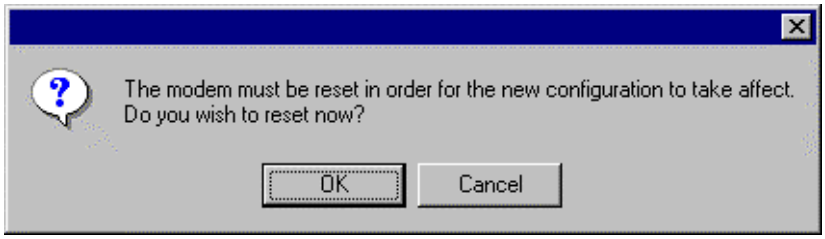
If you select **ETHERNET PORT 1**, the following pop-up will be displayed. Click on **OK.**


Microsoft Internet Explorer
This change will disable your DSL port. The WAN interface will be changed to ethernet port 1
OK

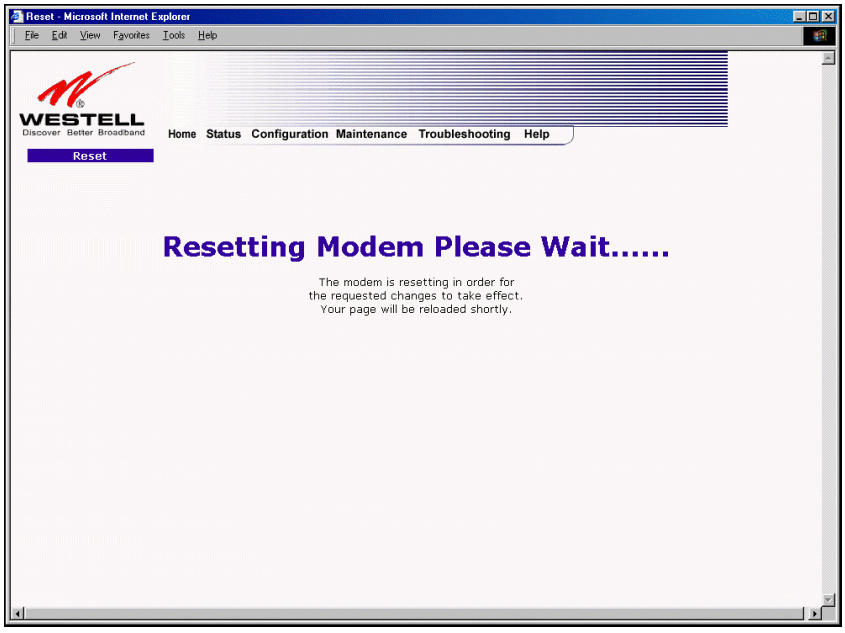
If you click on **OK**, the following pop-up screen will be displayed. Click on **OK.**



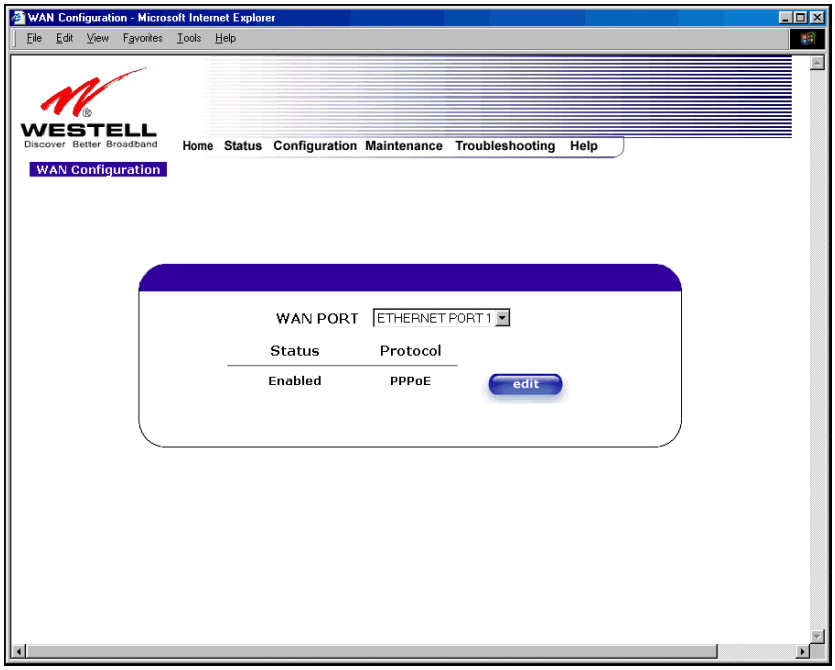
If you click on **OK** in the preceding pop-up screen, the following pop-up screen will be displayed. Click on **OK.** The modem will be reset to allow the configuration to take effect.



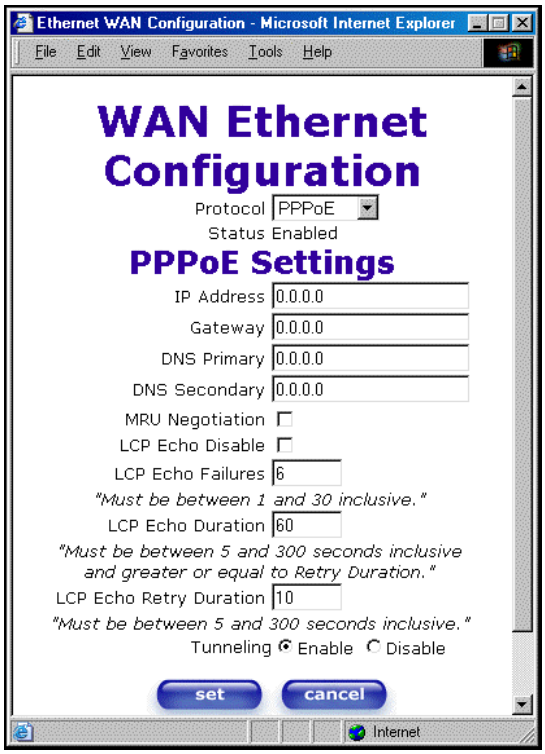
If you clicked on **OK,** VersaLink will be reset and the new configuration will take effect.


Reset - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Reset
Resetting Modem Please Wait.....
The modem is resetting in order for
the requested changes to take effect.
Your page will be reloaded shortly.

After the Gateway has been reset, select **Advanced WAN > WAN** from the **Configuration** menu. The following screen will be displayed. To configure the WAN PORT **"ETHERNET PORT 1"** settings, click edit.

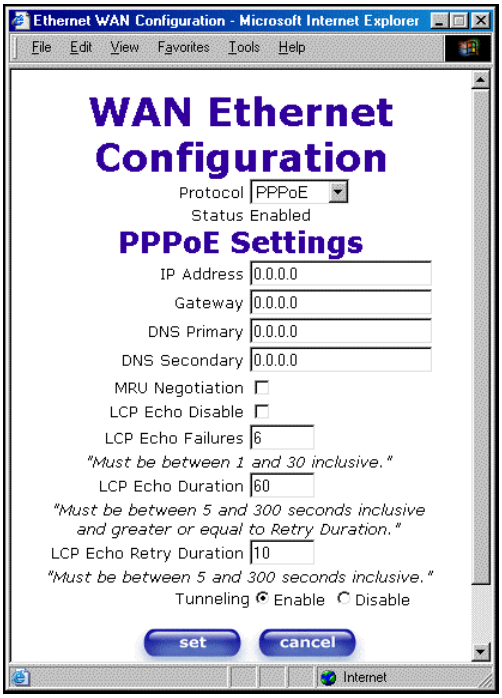


If you clicked **edit,** the following screen will be displayed. By using this screen, you can configure the WAN Ethernet port settings of your Gateway.

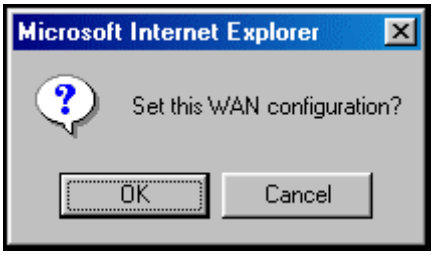

Ethernet WAN Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WAN Ethernet Configuration
Protocol PPPoE
Status Enabled
PPPoE Settings
IP Address 0.0.0.0
Gateway 0.0.0.0
DNS Primary 0.0.0.0
DNS Secondary 0.0.0.0
MRU Negotiation
LCP Echo Disable
LCP Echo Failures 6
"Must be between 1 and 30 inclusive."
LCP Echo Duration 60
"Must be between 5 and 300 seconds inclusive and greater or equal to Retry Duration."
LCP Echo Retry Duration 10
"Must be between 5 and 300 seconds inclusive."
Tunneling Enable Disable
set cancel
Internet

13.6.3.4.1 Configuring WAN Ethernet for PPPoE

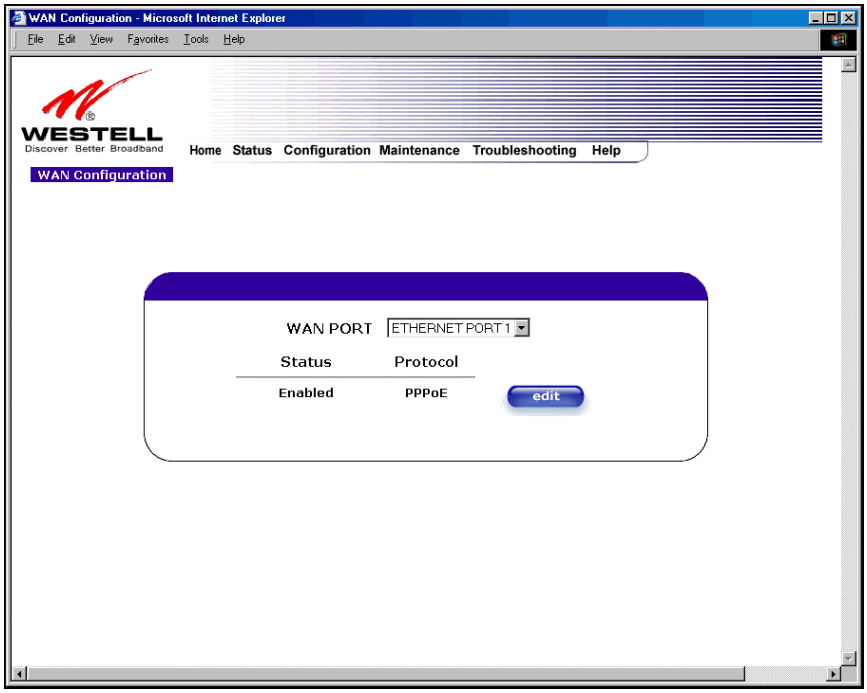
To configure the WAN Ethernet port for PPPoE protocol, select **PPPoE** from the **Protocol** drop-down menu. Enter the appropriate values in the fields, and then click **set VC** to save the settings.


Ethernet WAN Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WAN Ethernet Configuration
Protocol PPPoE
Status Enabled
PPPoE Settings
IP Address 0.0.0.0
Gateway 0.0.0.0
DNS Primary 0.0.0.0
DNS Secondary 0.0.0.0
MRU Negotiation
LCP Echo Disable
LCP Echo Failures 6
"Must be between 1 and 30 inclusive."
LCP Echo Duration 60
"Must be between 5 and 300 seconds inclusive and greater or equal to Retry Duration."
LCP Echo Retry Duration 10
"Must be between 5 and 300 seconds inclusive."
Tunneling Enable Disable
set
cancel
Internet

If you clicked the **set VC** button, the following pop-up screen will be displayed. Click on **OK** in the pop-up screen. If you click on **Cancel**, the new settings will not be saved. After you click on **OK,** follow the instructions to reset the Gateway, as previously discussed in section 13.6.3.

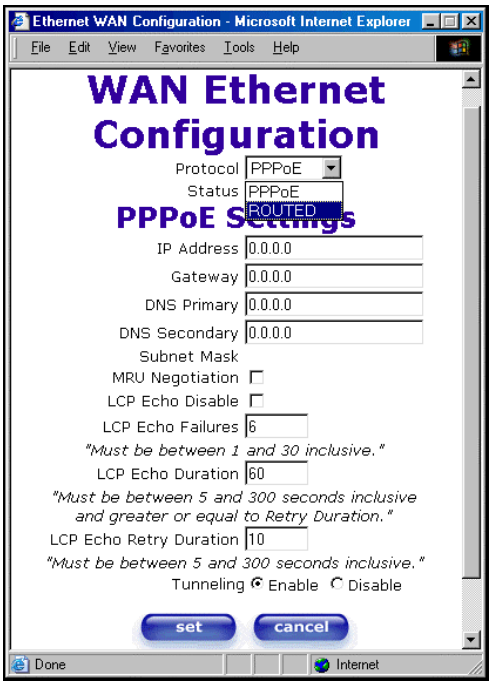


After the Gateway has been reset, the **WAN Configuration** screen will display **PPPoE** as the protocol for **ETHERNET PORT 1.**

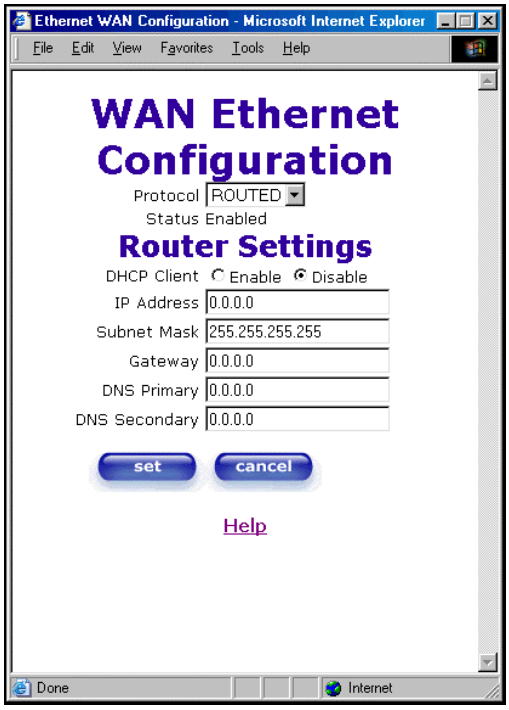


13.6.3.4.2 Configuring WAN Ethernet for Routed

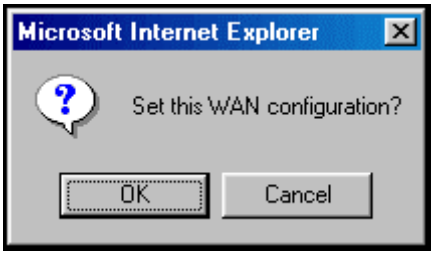
To configure the WAN Ethernet port for routed bridge protocol, select **ROUTED** from the **Protocol** drop-down menu. Enter the appropriate values in the fields, and then click **set VC** to save the settings.



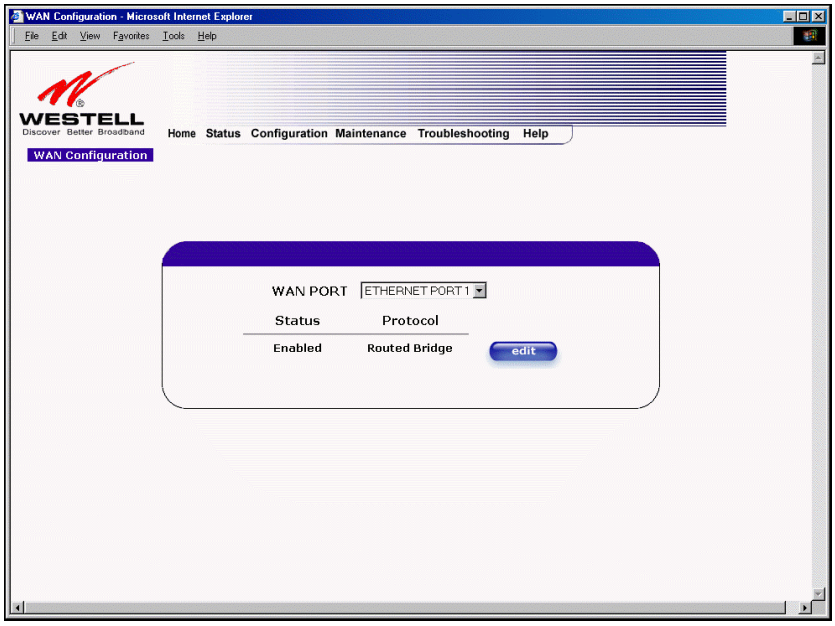
If you selected **ROUTED,** the following screen will be displayed. Enter the appropriate values in the fields and click **set.**



If you clicked **set**, the following pop-up screen will be displayed. Click **OK** in the pop-up screen. If you click **Cancel**, the new settings will not be saved. After you click on **OK,** follow the instructions to reset the Gateway, as previously discussed in section 13.6.3.

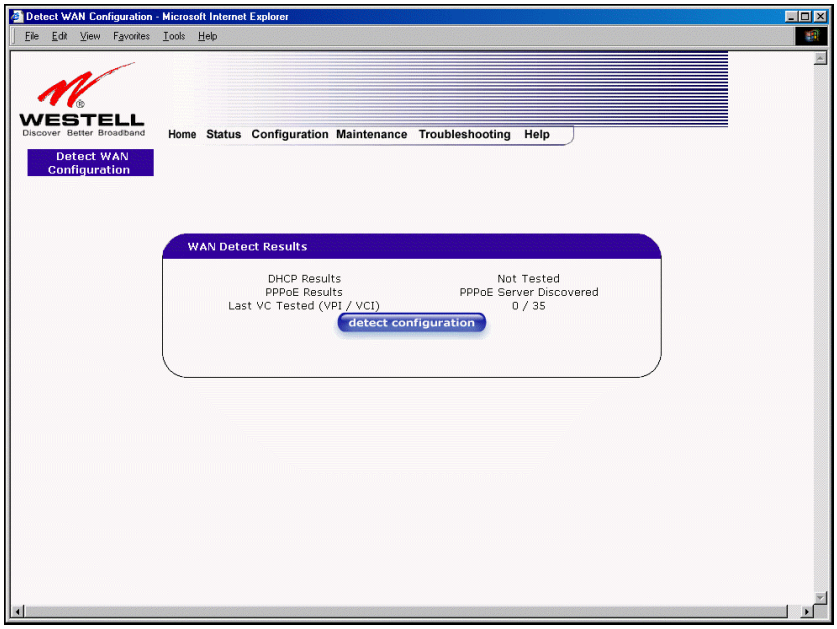


After the modem has been reset, the **WAN Configuration** screen will display **Routed Bridge** as the protocol for **ETHERNET PORT 1.**



13.6.4 WAN Detection

The following screen will be displayed if you select **Advanced WAN > WAN Detection** from the **Configuration** menu. If you click the **detect configuration** button, VersaLink will initiate automatic detection of the WAN protocol per VPI/VCI settings. The process detects DHCP-Enabled Routed Bridge or PPPoE Protocols.

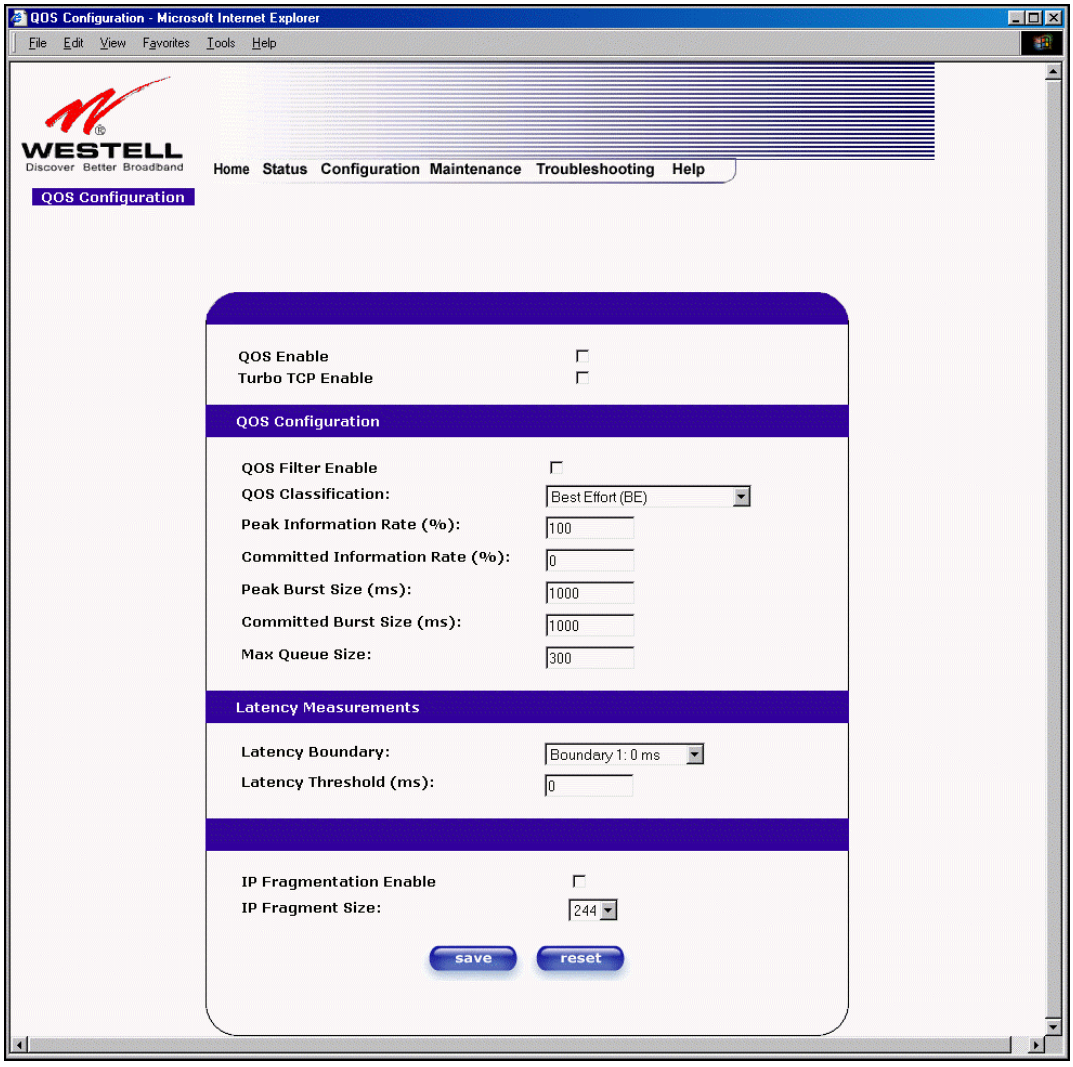

Detect WAN Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Detect WAN Configuration
WAN Detect Results
DHCP Results Not Tested
PPPoE Results PPPoE Server Discovered
Last VC Tested (VPI / VCI) 0 / 35
detect configuration

13.6.5 QOS

The following screen will be displayed if you select **Advanced WAN > QOS** from the **Configuration** menu. If you change any settings in this screen, click on **save.** If you click on **reset,** this screen will refresh and display your last saved QoS configuration.

NOTE: If VersaLink is configured using **ETHERNET PORT 1**, the following screen will not be available.

The QOS feature helps ensure data integrity in high-speed transmissions. QOS provides the capability to partition network traffic into multiple priority levels or classes of service. After packet classification, other QOS features can be utilized to assign the appropriate traffic handling policies including congestion management, bandwidth allocation, and delay bounds for each traffic class.

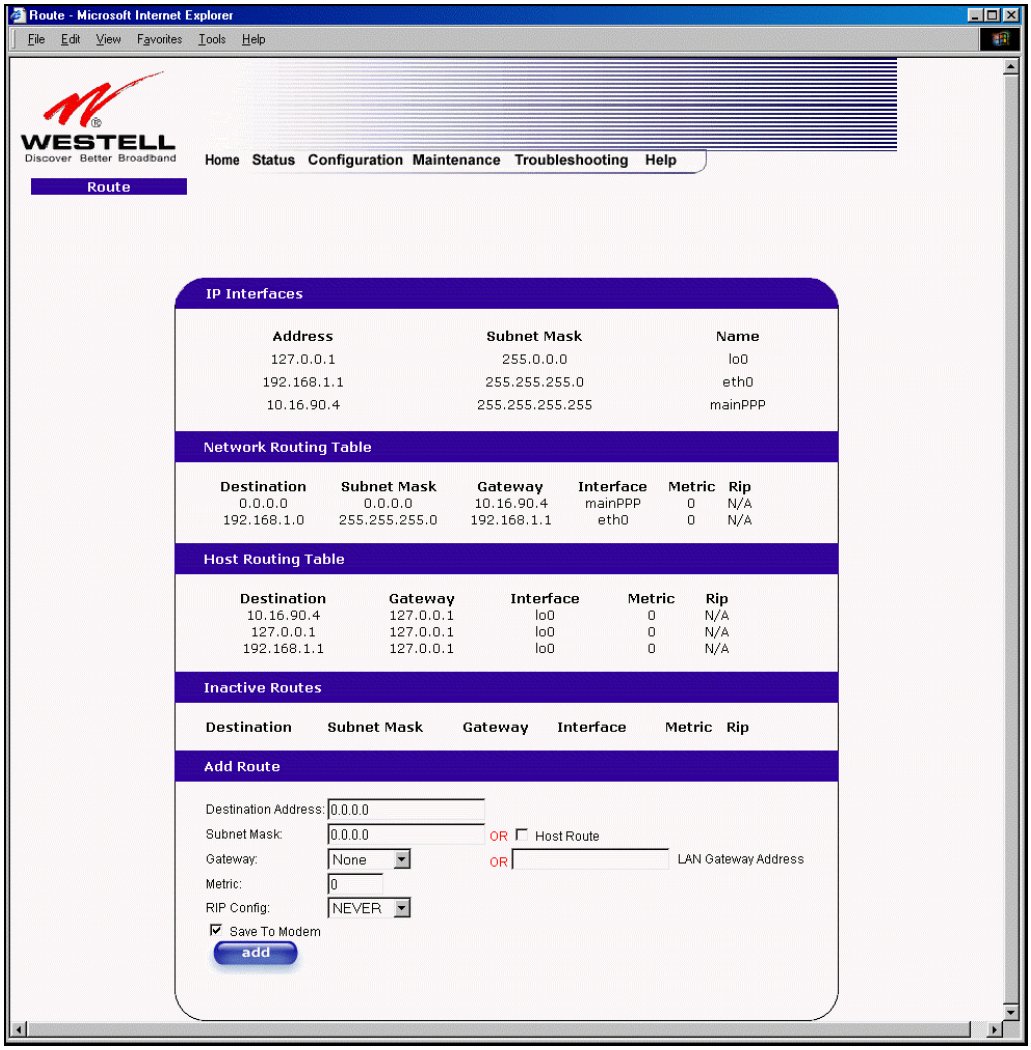


QOS Enable	Factory Default = DISABLED If this box is checked, Quality of Service (QOS) will be Enabled.
Turbo TCP Enable	Factory Default = DISABLED If this box is checked, Turbo TCP will be Enabled.
QOS Configuration	
QOS Filter Enable	Factory Default = DISABLED If this box is checked, this will Enable the QOS filter.
QOS Classification	This feature provides the capability to partition network traffic into multiple priority levels or classes of service. After packet classification, other QoS features can be utilized to assign the appropriate traffic handling policies including congestion management, bandwidth allocation, and delay bounds for each traffic class. Possible responses are: Best Effort (BE) Assured Forwarding (AF1) Assured Forwarding (AF2) Assured Forwarding (AF3) Assured Forwarding (AF4) Expedited Forwarding (EF) Network Control (NC)
Peak Information Rte (%)	The maximum allowed rate for this priority, expressed as a % of the DSL rate.
Committed Information Rate (%)	The committed rate for this priority, expressed as a % of the DSL rate.
Peak Burst Size	The interval in milliseconds for averaging the peak offered rate.
Committed Burst Size	The interval in milliseconds for averaging the committed offered rate.
Max Queue Size	The number of packets that can be queued for this priority.
Latency Measurements	
Latency Boundary	This configures the maximum latency boundary in milliseconds that a specific packet may be delayed by.
Latency Threshold (ms)	This setting configures the maximum latency boundary in milliseconds that a specific packet may be delayed by. Possible responses are: Boundary 1:0 ms Boundary 2:10 ms Boundary 3:30 ms Boundary 4:40 ms Boundary 5:100 ms Boundary 6:1000 ms Boundary 7:3000 ms
IP Fragmentation Enable	Factory Default = DISABLED If this box is checked, IP Fragmentation will be Enabled. If Enabled and packets larger than 1500 bytes total are received, they will be fragmented.
IP Fragment Size	This is the IP Packet Size. Possible responses are: 100, 148, 244, 292, 340, 388, or 436

If you made changes to the **QOS Configuration** and clicked on **save,** the following screen will be displayed. Click **OK** to save your new QOS settings.

13.6.6 Route

The following screen will be displayed if you select **Advanced WAN > Route** from the **Configuration** menu. The Route table maintains the routes or paths of where specific types of data shall be routed across a network. To add a Route, enter the appropriate values and/or select the desired options in this screen, and then click **add** to establish a static route.



Note: In this screen, VersaLink represents 'Gateway.'

IP Interfaces	
IP Interfaces	The list of active interfaces on the modem and their IP and Subnet mask address. Eth0 is the local LAN interface. Lo0 is the loopback interface. MainPPP is the local WAN interface.
Address	The IP interface address.
Subnet Mask	The IP interface subnet address.
Name	The IP interface device name.
Network Routing Table	
Network Routing Table	The list of network routes. These can be either routes for directly connected interfaces or static routes.
Destination Address	The IP address or subnet of the Route.
Subnet Mask	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
VersaLink	Indicates were to send the packet if it matches this route.
Interface	Indicates were to send the packet if it matches this route.
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP	Indicates whether a static route should be advertised via RIP.
Host Routing Table	
Host Routing Table	The list of host routes. A host route is an IP route with a 32-bit mask, indicating a single destination (as opposed to a subnet, which could match several destinations.)
Destination Address	The IP address or subnet of the Route.
Subnet Mask	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
VersaLink	Indicates were to send the packet if it matches this route.
Interface	Indicates were to send the packet if it matches this route.
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP	Indicates whether a static route should be advertised via RIP.
Inactive Routes	
Inactive Routes	Static routes whose interface is currently not in service.
Destination Address	The IP address or subnet of the Route.
Subnet Mask	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
VersaLink	Indicates were to send the packet if it matches this route.
Interface	Indicates were to send the packet if it matches this route.
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP	Indicates whether a static route should be advertised via RIP.
Add Route	
Add Route	This is used to add a new static route in the modem.
Destination Address	The IP address or subnet of the Route.
Subnet Mask/ Host Route	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
VersaLink/IP Address	The interface to use for sending the packet, if it matches this route. (Only active VersaLinks can be used to create a static route.)
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP Conf	Determines whether or not to advertise the static route, using RIP. (RIP must also be enabled before the route will be advertised.)
Save to Modem	If checked, then the route will be made permanent by saving it to flash memory. If not checked, the route will disappear the next time the modem restarts.

13.6.7 RIP

The following details will be displayed if you select **Advanced WAN > RIP** from the **Configuration** menu. If you change any settings in this screen, click on **save.** If you click on **reset,** this screen will refresh and display your last saved RIP configuration.

RIP (Routing Interface Protocol) is a dynamic inter-network routing protocol primarily used in interior routing environments. A dynamic routing protocol, as opposed to a static routing protocol, automatically discovers routes and builds routing tables.

Note: In this screen, VersaLink represents 'Gateway.'

RIP Enable	Factory Default = DISABLED If this box is checked, RIP will be Enabled (turned ON).
RIP Configuration	
Interface Type	LAN: Select this if you are configuring RIP for the LAN side. WAN: Select this if you are configuring RIP for the WAN side. (WAN side is receive only.)
Receive	The version of RIP to be accepted. Possible responses are: None RIPv1 RIPv2 RIPv1 or RIPv2
Transmit	The version of RIP to be transmitted. (WAN side RIP never transmits) Possible responses are: None RIPv1 RIPv1 Compatible RIPv2
RIPv2 Authentication Mode	If using RIP V2, you must select the type of authentication to use. Possible responses are: None Clear Text MD5 (If MD5 authentication, the password)
Advanced	
Default VersaLink	Factory Default = DISABLED If this box is check (Enabled), this feature will determine whether the modem advertises itself as a VersaLink (i.e., the default route)
Border VersaLink Filtering	Factory Default = ENABLED If this box is unchecked (Disabled), the modem will not summarize subnets into a single route before advertising.
RIP Timer Rate	Indicates how often to update the local routing table.
RIP Supply Interval	Indicates how often to advertise routes to neighbors.
RIP Expire Time	Indicates how long routes received from neighbors become invalid, if no refresh of the route is received.
RIP Garbage Collection Time	Indicates how long to advertise invalid routes after they have expired.

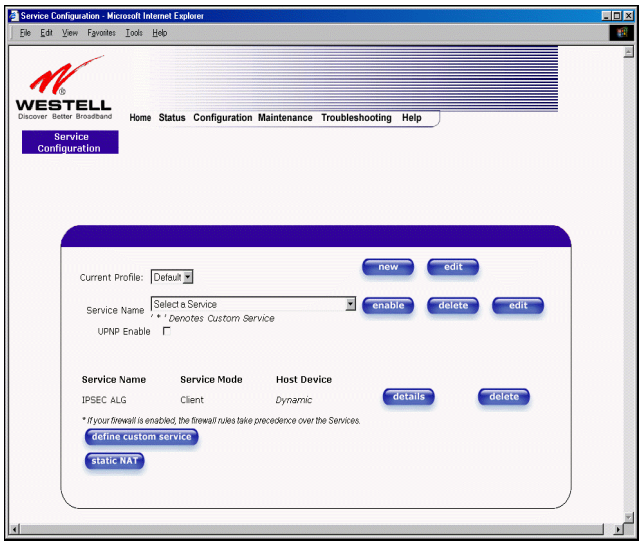
If you change any settings in the **RIP Configuration** screen and click on **save,** the following screen will be displayed. Click on **OK** to save your new RIP settings.

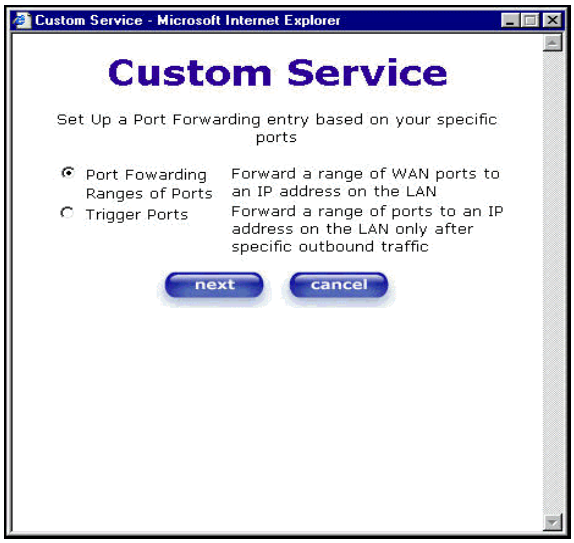
14. SETTING UP ADVANCED SERVICE CONFIGURATION

You can set up additional Service Configuration options for VersaLink that allow you to enter the port forwarding and trigger ports ranges of your choice. Select **Services** from the **Configuration** menu. The **Service Configuration** screen will be displayed.

If you click **define custom service** in the **Service Configuration** screen, the **Custom Service** screen will guide you through the steps of creating an advanced NAT services via port forwarding and/or trigger port configuration.

NOTE: Westell strongly recommends that you do not change any values in this section. If you experience any problems, please reset VersaLink via the external hardware reset button or the procedure defined under the Maintenance menu explained in section 15 of this User Guide.


Service Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Service Configuration
Current Profile: Default
new edit
Service Name Select a Service
* Denotes Custom Service
enable delete edit
UPNP Enable
Service Name Service Mode Host Device
IPSEC ALG Client Dynamic
details delete
* If your firewall is enabled, the firewall rules take precedence over the Services.
define custom service
static NAT

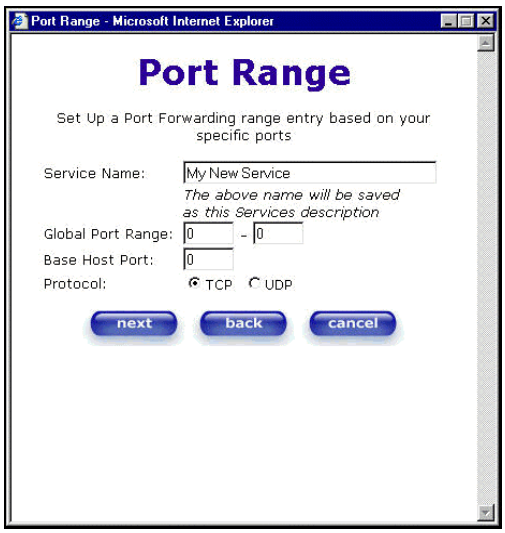

Custom Service - Microsoft Internet Explorer
Custom Service
Set Up a Port Forwarding entry based on your specific ports
Port Fowarding Ranges of Ports
Forward a range of WAN ports to an IP address on the LAN
Trigger Ports
Forward a range of ports to an IP address on the LAN only after specific outbound traffic
next
cancel

Port Forwarding Ranges of Ports	This option allows you to forward a range of WAN ports to an IP address on the LAN.
Trigger Ports	This option allows you to forward a range of ports to an IP address on the LAN only after specific outbound traffic.

14.1 Port Forwarding Ranges of Ports

To select **Port Forwarding Ranges of Ports**, click on **define custom service** from the **Service Configuration** screen, and then select **Port Forwarding Ranges of Ports** from the **Custom Service** screen. Click **Next**. The **Port Range** screen will be displayed. Enter your Port Range values in the fields provided, and click **next** to continue.

Custom Service - Microsoft Internet Explorer
Custom Service
Set Up a Port Forwarding entry based on your specific ports
Port Fowarding Ranges of Ports
Forward a range of WAN ports to an IP address on the LAN
Trigger Ports
Forward a range of ports to an IP address on the LAN only after specific outbound traffic
next
cancel



14.2 Adding Port Forwarding Ports

If you made changes in the **Port Range** screen and clicked on **next**, the following screen will be displayed. Click on **close** to accept the changes, or click on **add** to go back to **Port Range** screen and enter additional port range values. You can repeat this step for each range of ports that you want to add (up to 62 port forwarding ranges). When you have finished adding ports, click **close** to accept the changes and to return to the **Service Configuration** screen.

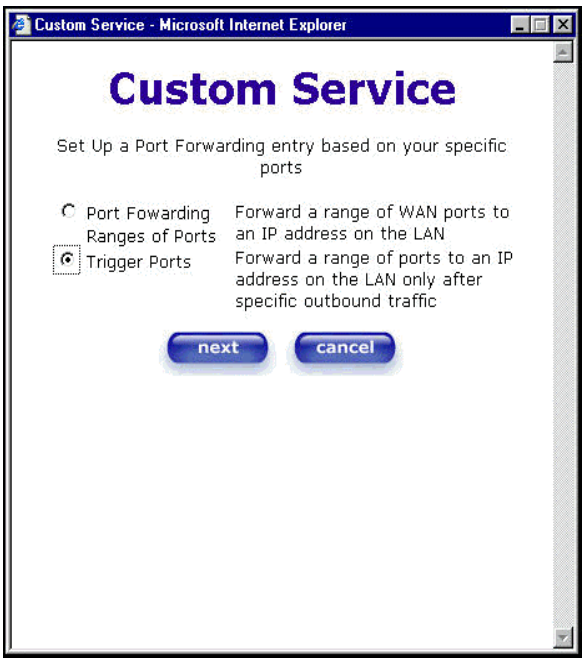
IMPORTANT: After you click close, return to the **Service Configuration** screen and, from the drop-down menu, select the service that you used in your port range configuration. Then, click **enable** to allow the settings to take effect. Note: In this example, **My New Service** is the service name used in this port range configuration.

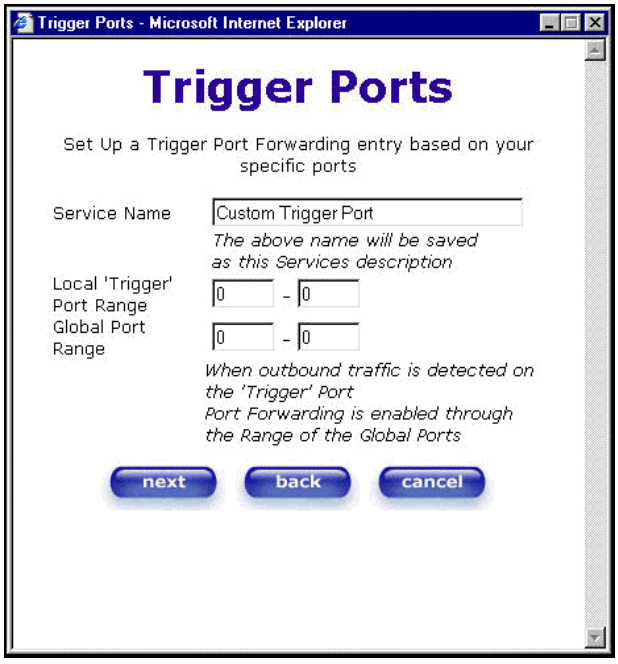
Service Details - Microsoft Internet Explorer
Service Details
Service Name *My New Service
Type Port Forwarding
Port 1
Protocol: TCP
Global Port(s): 2-20
Base Host Port: 2
add
After clicking 'Close' you can enable your new service from the 'Serivce Name' select box.
close

Service Name	The NAT service for which you are configuring Port Forwarding.
Type	The type of NAT service configuration you selected.
Protocol	The type of Protocol that is used to run this NAT service. TCP - Transmission Control Protocol. UDP - User Datagram Protocol (UDP).
Global Ports	The WAN-side TCP/UDP port range.
Base Host Port	The port on the WAN that will host the NAT service selected. Base Host Port is the first port that will be used for a specific service when configured for a range of ports.

14.3 Port Forwarding Trigger Ports

To select **Port Forwarding Trigger Ports**, click **define custom service** in the **Service Configuration** screen, and then select **Trigger Ports** from the **Custom Service** screen. Click on **next**. The follow settings will be displayed in the **Trigger Ports** screen. Enter your Trigger Port values in the fields provided, and click on **next** to continue.


Custom Service - Microsoft Internet Explorer
Custom Service
Set Up a Port Forwarding entry based on your specific ports
Port Fowarding Ranges of Ports
Forward a range of WAN ports to an IP address on the LAN
Trigger Ports
Forward a range of ports to an IP address on the LAN only after specific outbound traffic
next
cancel


Trigger Ports - Microsoft Internet Explorer
Trigger Ports
Set Up a Trigger Port Forwarding entry based on your specific ports
Service Name
Custom Trigger Port
The above name will be saved as this Services description
Local 'Trigger' Port Range
Global Port Range
When outbound traffic is detected on the 'Trigger' Port
Port Forwarding is enabled through the Range of the Global Ports
next
back
cancel

Service Name	The NAT service you selected.
Local Trigger Port Range	The local LAN side TCP/UDP port.
Global Port Range	The WAN side TCP/UDP port range.

14.4 Adding Local Trigger Ports

If you made changes in the **Local 'Trigger' Port Range** screen and clicked **next**, the following screen will be displayed. Click **close** to accept the changes, or click **add** to go back to the **Trigger Ports** screen and enter additional values. You can repeat this step for each port range that you want to add (up to 10 trigger ports). When you have finished adding ports, click **close** to accept the changes and to return to the **Service Configuration** screen.

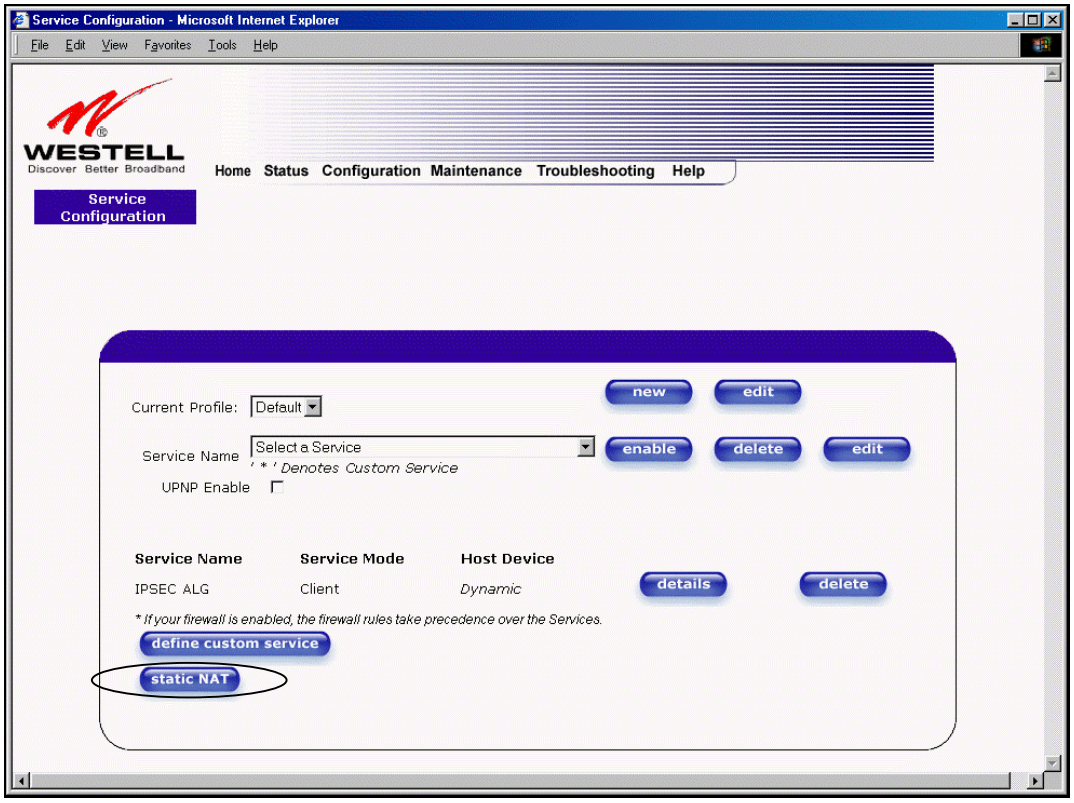
IMPORTANT: After you click close, return to the **Service Configuration** screen and, from the drop-down menu, select the service that you used in your trigger port configuration. Then, click **enable** to allow the settings to take effect. Note: In this example, **Custom Trigger Port** is the service name used in this trigger port configuration.

14.5 Static NAT

If you select **Services** from the **Configuration** menu, the following screen will be displayed, showing the **static NAT** button. Static NAT allows you to configure VersaLink to work with the special NAT services.

NOTE: When VersaLink is configured for Static NAT, any unsolicited packets arriving at the WAN would be forwarded to this device. This feature is used in cases where the user wants to host a server for a specific application.

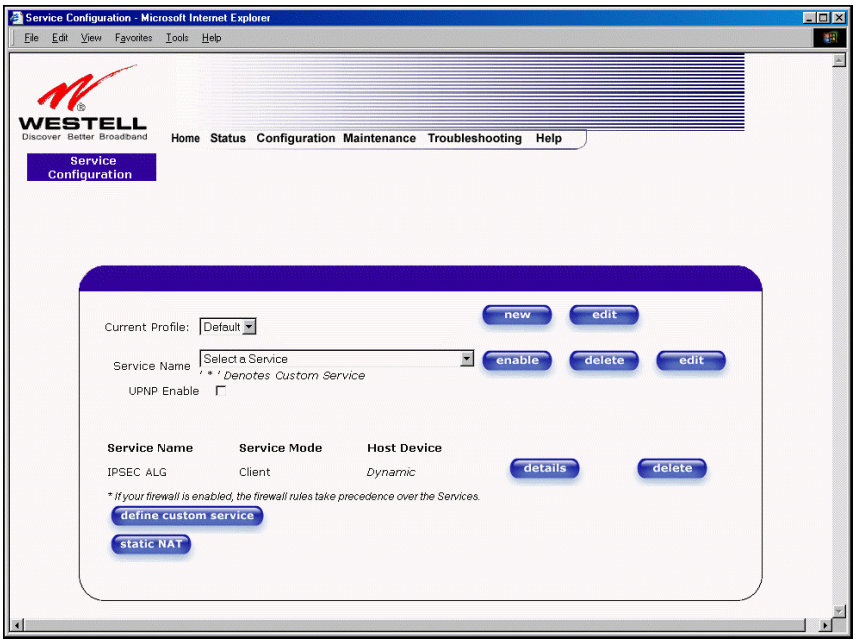
STOP: Single Static IP should be disabled (if it has been enabled previously) before you enable **static NAT**. To disable Single Static IP, select **Single Static IP** from the **Configuration** menu. Next, click on the **disable** button, and then click on **OK** in the pop-up screens to allow the Gateway to be reset. As explained in section 13.1 (Single Static IP), you must reboot your computer after you enable or disable Single Static IP. After you have rebooted your computer, return to static NAT configuration screen by selecting **Services** from the **Configuration** menu and then by clicking the **static NAT** button.


Service Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Service Configuration
Current Profile: Default
new edit
Service Name Select a Service
enable delete edit
' * ' Denotes Custom Service
UPNP Enable
Service Name Service Mode Host Device
IPSEC ALG Client Dynamic
details delete
* If your firewall is enabled, the firewall rules take precedence over the Services.
define custom service
static NAT

14.6 Enabling Static NAT

Before you enable static NAT, select **Default** from the **Current Profile** drop-down box. Static NAT must be configured for the Gateway's default account profile. After you select the default profile, click the **static NAT** button.

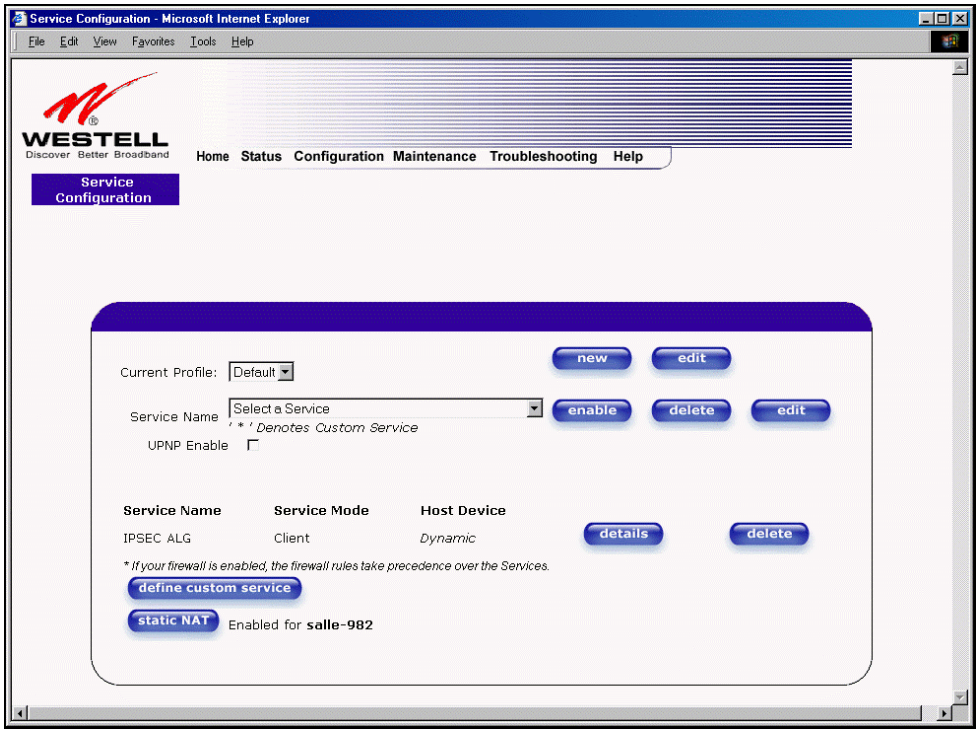
NOTE: In the following screen, the default account profile is labeled **Default**. However, if you have renamed the default account profile, you must select the profile name you created as the default profile.


Service Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Service Configuration
Current Profile: Default
new edit
Service Name Select a Service
enable delete edit
' * ' Denotes Custom Service
UPNP Enable
Service Name Service Mode Host Device
IPSEC ALG Client Dynamic
details delete
* If your firewall is enabled, the firewall rules take precedence over the Services.
define custom service
static NAT

If you click on the **static NAT** button in the **Service Configuration** screen, the following screen will be displayed. Select a device from the **Static NAT Device** drop-down arrow, or type the IP address of the device in the field labeled **IP Address**. Click on **enable**. This will automatically enable the Static NAT feature for that device.

Static NAT - Microsoft Internet Explorer
Static NAT
Set Up an IP Address to be your Default NAT Destination.
Static NAT Device salle-982
or specify
IP Address
All unsolicited inbound traffic will be sent to the above device.
Note: Static Nat and IP Passthrough are mutually exclusive features.
enable disable cancel

If you click **enable,** the following **Service Configuration** screen will display. Static NAT is now enabled for the device you selected.

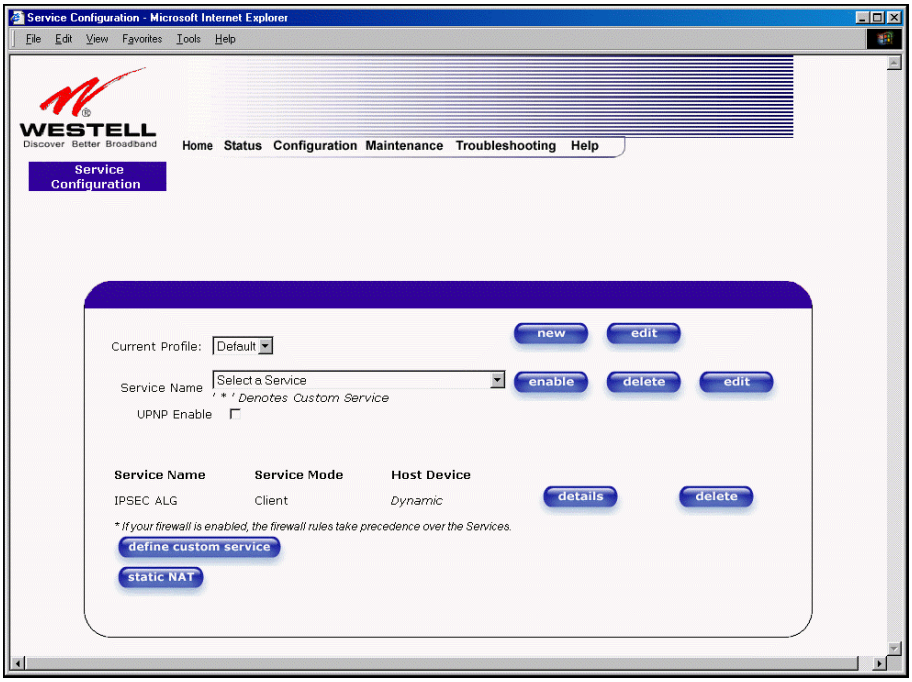

Service Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Service Configuration
Current Profile: Default
new edit
Service Name Select a Service
' * ' Denotes Custom Service
enable delete edit
UPNP Enable
Service Name Service Mode Host Device
IPSEC ALG Client Dynamic
details delete
* If your firewall is enabled, the firewall rules take precedence over the Services.
define custom service
static NAT Enabled for salle-982

14.7 Disabling Static NAT

To disable Static NAT, select **static NAT** in the **Service Configuration** screen, the following screen will be displayed. Next, select a device name from the **Static NAT Device** drop-down arrow, or type the IP address of the device in the field labeled **IP Address.** Click **disable.** This will automatically disable the Static NAT feature for that device.

Static NAT - Microsoft Internet Explorer
Static NAT
Set Up an IP Address to be your Default NAT Destination.
Static NAT Device
salle-982
or specify
IP Address
All unsolicited inbound traffic will be sent to the above device.
Note: Static Nat and IP Passthrough are mutually exclusive features.
enable
disable
cancel

If you clicked **disable,** the following **Service Configuration** screen will be displayed. Static NAT is now disabled for the device you selected. (No device is displayed in the field adjacent to the **static Nat** button.)



15. MAINTENANCE

15.1 Backup/Restore

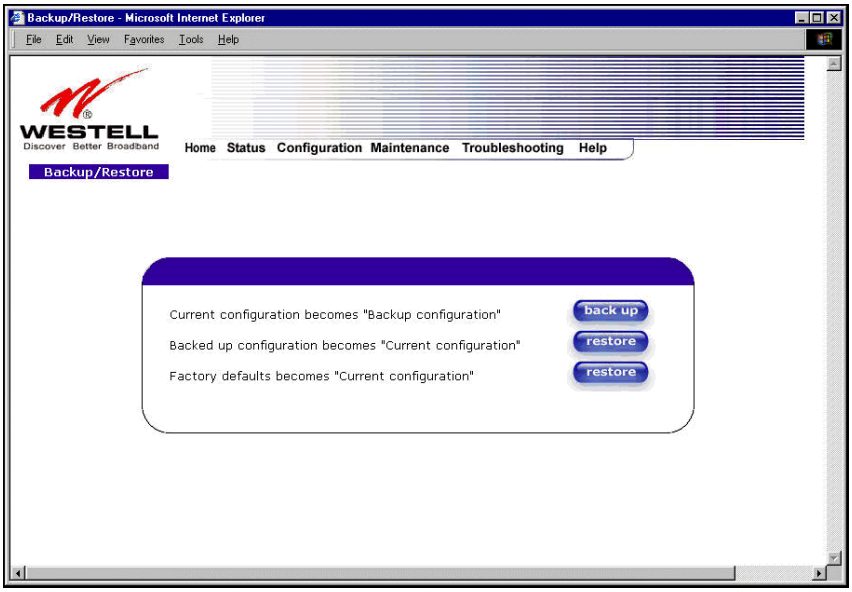
The following screen will be displayed if you select **Backup/Restore** from the **Maintenance** menu.

NOTE: Backup settings are stored in a separate area of flash, not to an external backup source.

Select one of the following options:

- **Current configuration becomes Backup Configuration:** Click **backup** to store the current configuration of your Gateway so that it can be recalled later.
- **Backed up configuration becomes current configuration:** Click **restore** if you want to retrieve the last back up copy of all configuration parameters and make these values current.
- **Factory default becomes Current configuration:** Click **restore** if you want set all user configurable parameters back to the factory default settings.

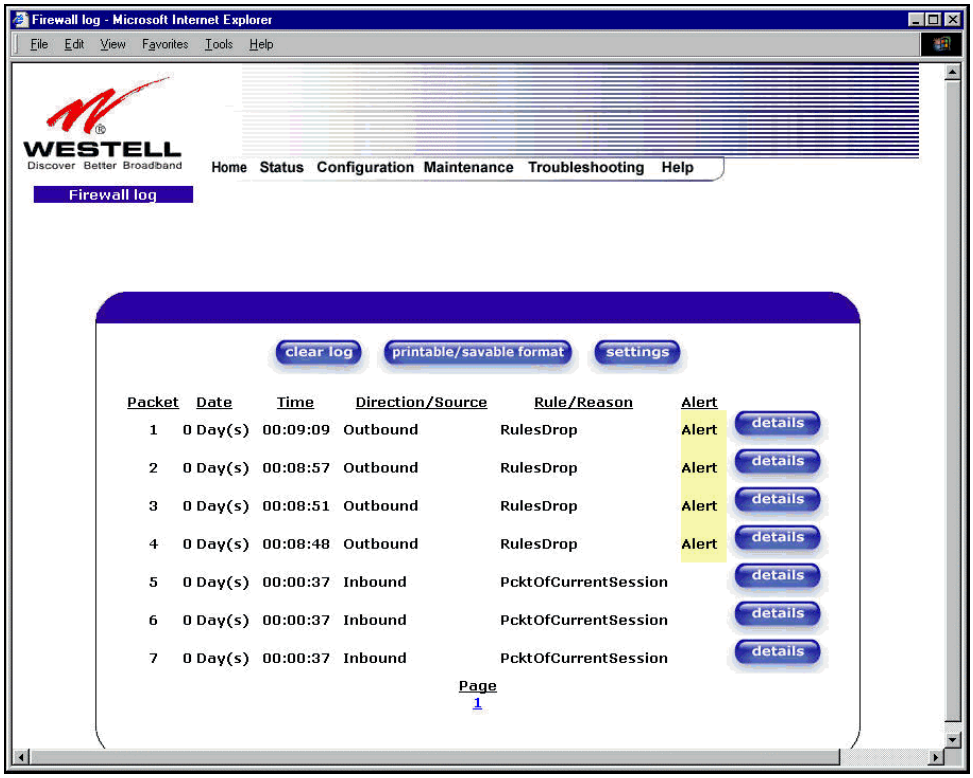
CAUTION: If you restore the Gateway to factory default settings, any data that the Gateway has reported will be lost.



15.2 Firewall Log

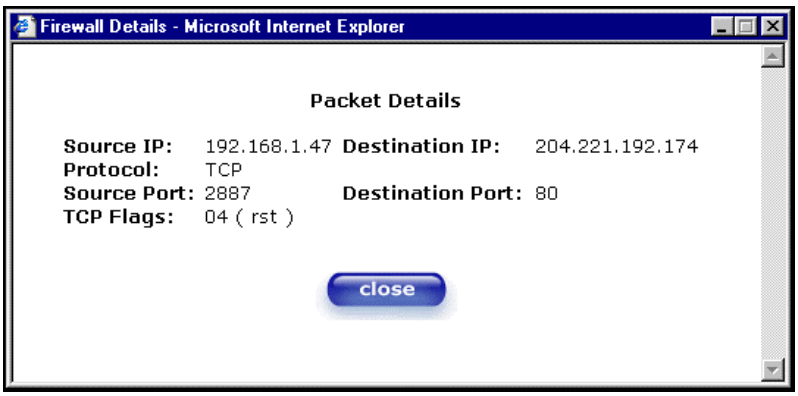
The following screen will be displayed if you select **Firewall Log** from the **Maintenance** menu.

This screen is an advanced diagnostics screen. It alerts you of noteworthy information sent to VersaLink from the Internet. The screen can contain 1000 entries, but a maximum of 50 entries are displayed at a time. Once 1000 entries have been logged, the oldest entry is removed to make space for the new entries as they occur.


Firewall log - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Firewall log
clear log
printable/savable format
settings
Packet Date Time Direction/Source Rule/Reason Alert
1 0 Day(s) 00:09:09 Outbound RulesDrop Alert details
2 0 Day(s) 00:08:57 Outbound RulesDrop Alert details
3 0 Day(s) 00:08:51 Outbound RulesDrop Alert details
4 0 Day(s) 00:08:48 Outbound RulesDrop Alert details
5 0 Day(s) 00:00:37 Inbound PcktOfCurrentSession details
6 0 Day(s) 00:00:37 Inbound PcktOfCurrentSession details
7 0 Day(s) 00:00:37 Inbound PcktOfCurrentSession details
Page
1

Clear log	Selecting this button removes all entries from the log.
Printable/savable format	Selecting this button opens a new window that contains a list of all the logged packets that can be saved or printed.
Settings	Selecting this button opens a new window that contains configuration settings for selecting the information that you want logged.
Packet	The packet number.
Date	The number of days passed since that the packet was sent.
Time	The time that the packet was sent.
Direction/Source	The direction of transmission.
Rule/Reason	The internal rule that caused the logged event. The internal rule is set up under Firewall rules.
Alert	Displays a description of the logged event.

If you clicked on **details** in the **Firewall Log** screen, the **Packet Details** screen will be displayed. Click on **close.**


Firewall Details - Microsoft Internet Explorer
Packet Details
Source IP: 192.168.1.47 Destination IP: 204.221.192.174
Protocol: TCP
Source Port: 2887 Destination Port: 80
TCP Flags: 04 (rst)
close

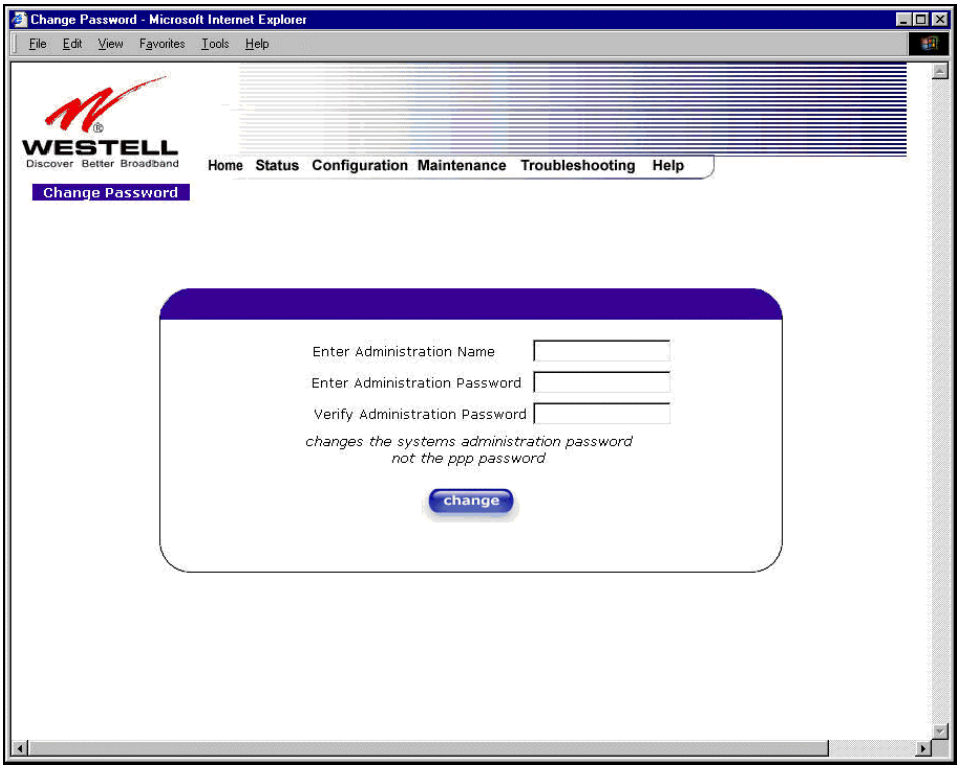
To clear the Firewall log, click **clear log** in the **Firewall Log** screen. The following pop-up screen will be displayed. Click **OK** when asked "**Do you wish to clear the Firewall log file?"** If you click **Cancel**, the firewall log will not be cleared.

To obtain a printable format of the Firewall Log, at the **Firewall Log** screen, click **Printable/Savable Format**. This will allow you to send a copy of the Firewall log to your designated printer.

15.3 Administrative Password

The following screen will be displayed if you select **Administrative Password** from the **Maintenance** menu. Enter your values in the appropriate fields and then click **change**.

NOTE: If the Gateway is password protected and you are not an authorized user, you will not be able to change the values. (The Gateway cannot be configured unless the user is logged in.) Contact your network administrator for further instructions.



Enter Administrative Name NOTE: This changes the Systems Administrator password not the PPP password.	Type the name of your network administrator.
Enter Administrative Password	Type your network administrator's password.
Verify Administrative Password	Retype your network administrator's password.

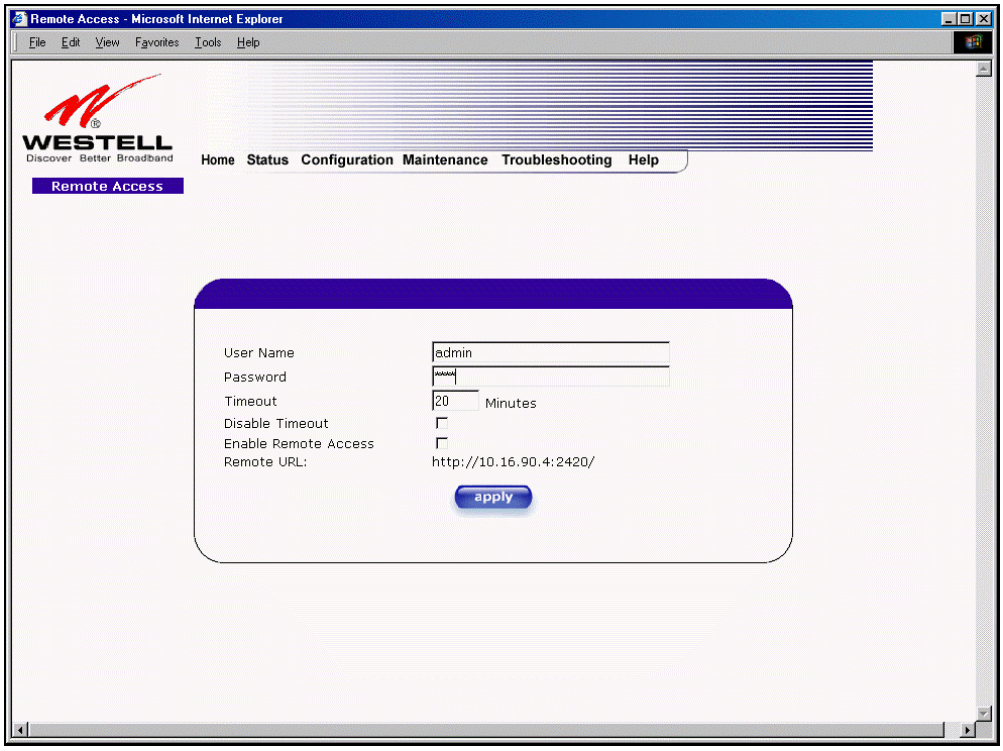
15.4 Remote Access

The following screen will be displayed if you select **Remote Access** from the **Maintenance** menu. To enable remote access, perform the following steps:

1. Enter the administrator's password.

   Note: The password should be at least 4 characters long and should not exceed 32 characters. Do not type a blank space or asterisks in the **Password** field. The password is case sensitive.

2. Click the **Enable Remote Access** box (a check mark will appear in the box).
3. Click **apply** to allow the settings to take effect.

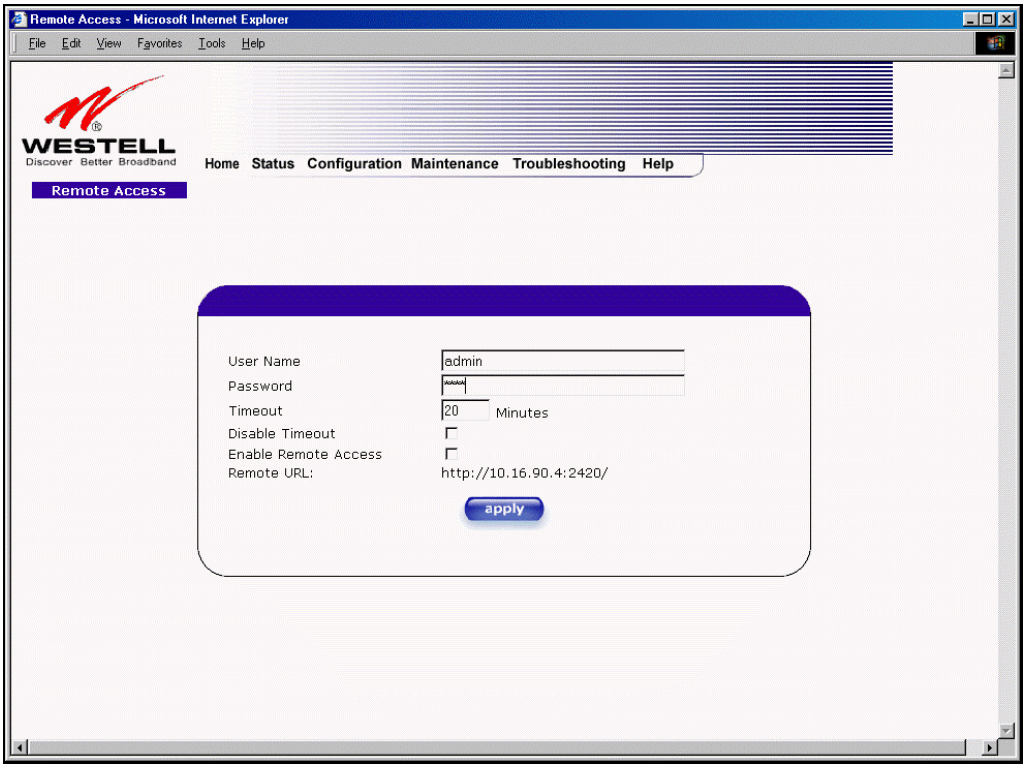


User Name	Displays your current User Name (Static field)
Password	Field for entering your password
Timeout	The number of minutes after which remote access will be deactivated (if it has been activated).
Disable Timeout	Click this box (a checkmark will appear) to activate the Disable Timeout feature. Uncheck the box to deactivate this feature.
Enable Remote Access	Click this box (a checkmark will appear) to activate Enable Remote Access. Uncheck the box to deactivate this feature.
URL	Displays the IP address of the remote management device (VersaLink).

After you enable Remote Access, the following message will be displayed:

> **Remote access is currently enabled. After 20 minutes of inactivity, or on reboot, remote access will be automatically disabled.**

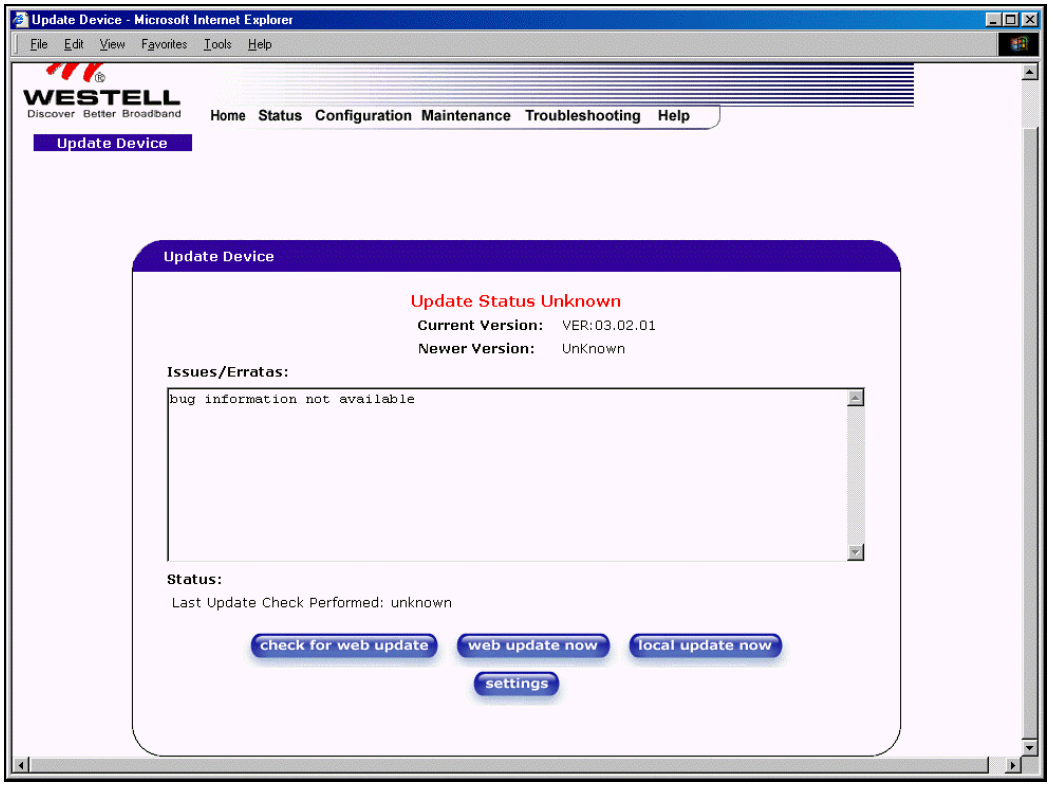
If you want to disable Remote Access, uncheck the **Enable Remote Access** box, and then click **apply** to save the settings.



15.5 Update Device

The following screen will be displayed if you select **Update Device** from the **Maintenance** menu. This screen is used to update the firmware that controls the operation of VersaLink. The updated firmware may be loaded from either a file that is located on your PCs hard drive or from update files stored on an Internet server.

CAUTION: The configurable settings of your Gateway may be erased during the update process.

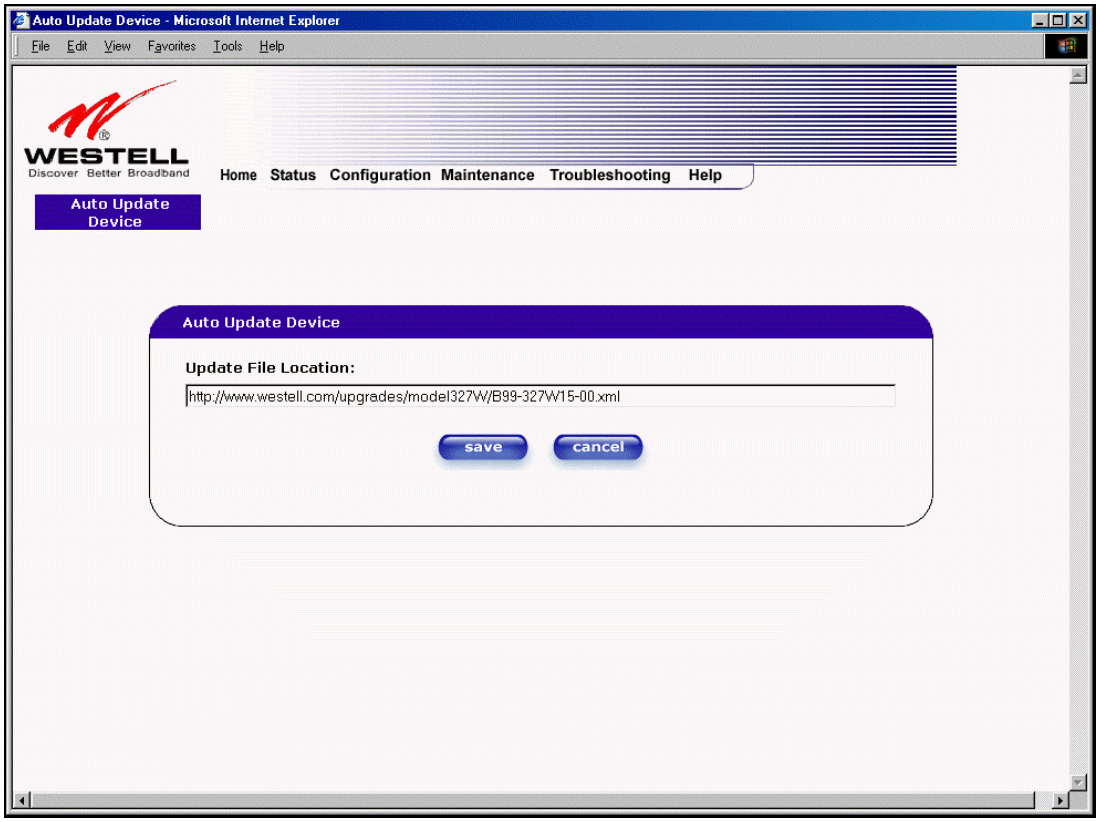


Click on the **check for web update** button in the **Update Device** screen to check the web for possible software updates. This screen will retrieve the software update file and display any available update information. You must be connected to the Internet to use this option.

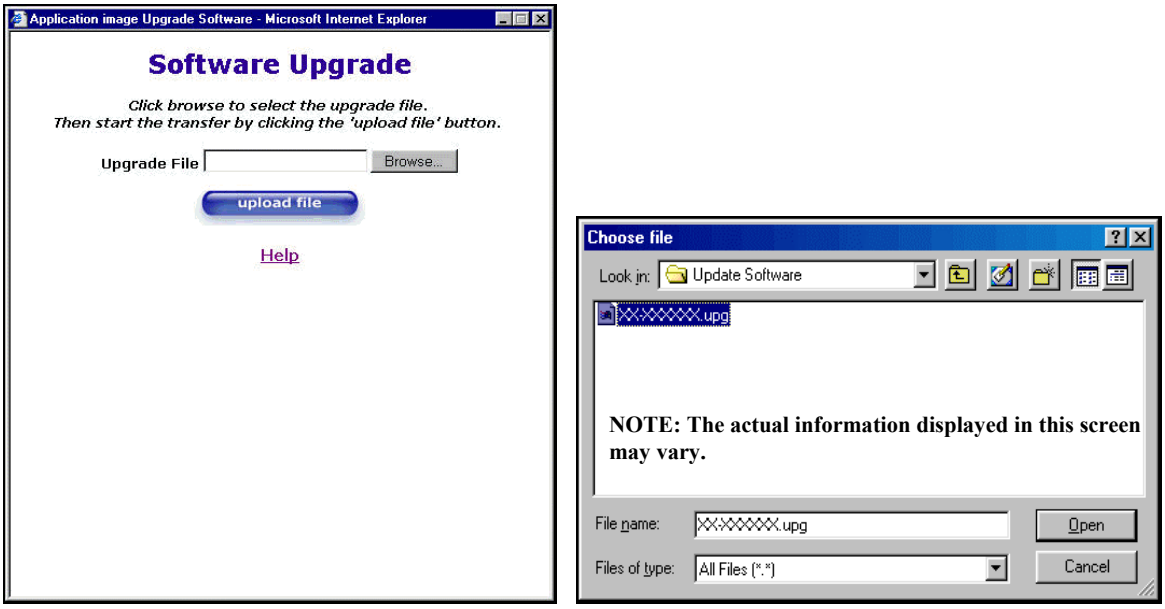
NOTE: If you click on check for web update and the page returns a “page not found” message, this indicates that the software update file is not available. Go back to the previous screen to continue.

Click on the **web update now** button in the **Update Device** screen to download the software update file and automatically update the modem firmware if an update is available and applicable. You must be connected to the Internet to use this option.

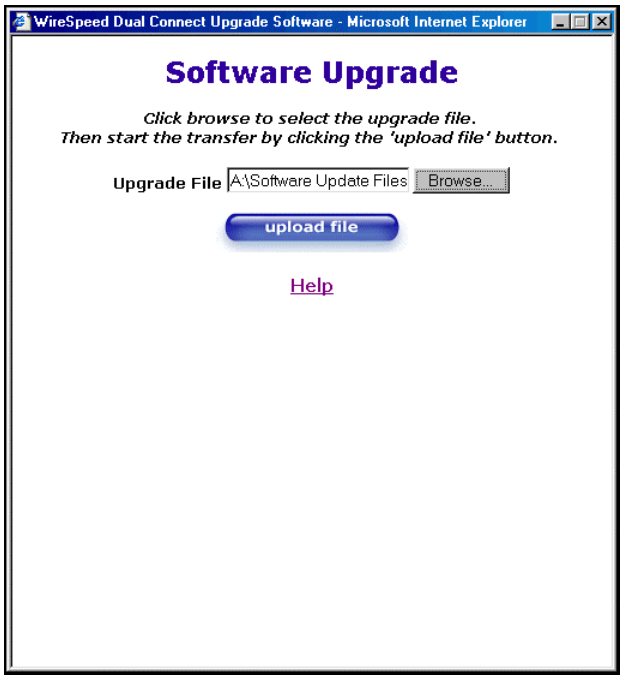
If you click on the **settings** button in the **Update Device** screen, the following screen will appear. This screen displays the location of the software update file.



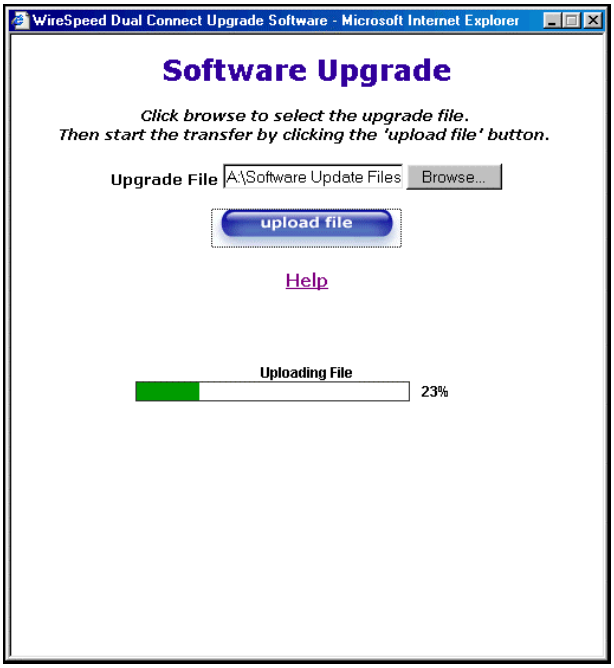
Click on the **local update now** button in the **Update Device** screen to select the upgrade file from your PC's hard drive. This screen allows you to upgrade the software on VersaLink. Click **Browse…** and go to the location where the upgrade file is stored.



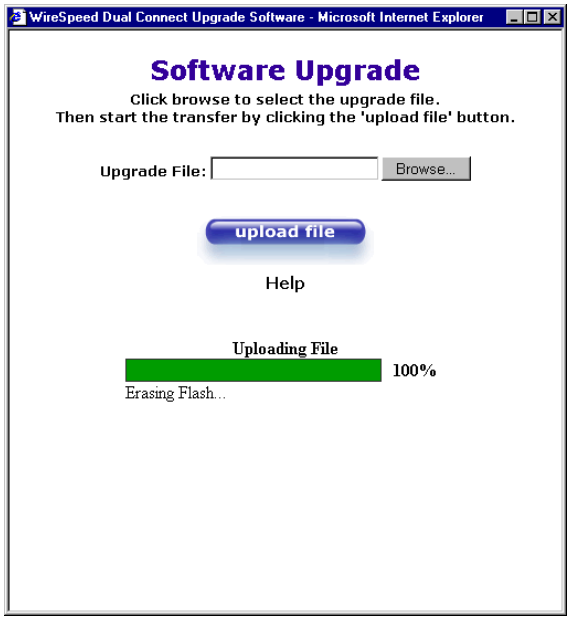
Select the appropriate upgrade file from your browser. The file name will appear in the field labeled **Upgrade File**. Click **upload file.**

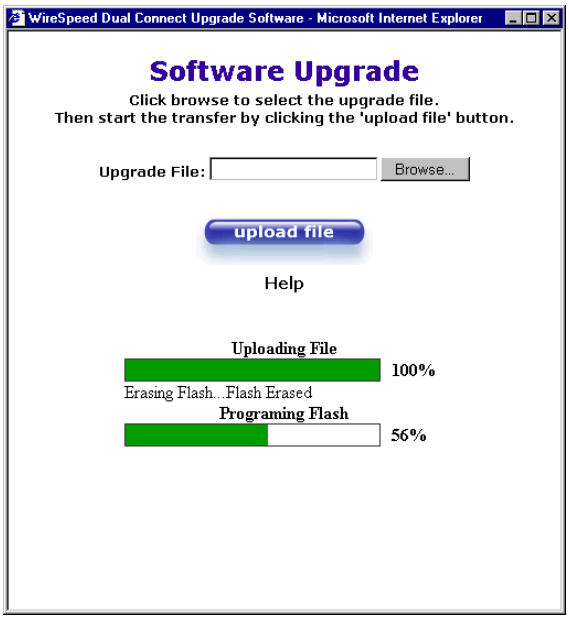

WireSpeed Dual Connect Upgrade Software - Microsoft Internet Explorer
Software Upgrade
Click browse to select the upgrade file.
Then start the transfer by clicking the 'upload file' button.
Upgrade File
A:\Software Update Files
Browse...
upload file
Help

This screen shows that the file is being uploaded to VersaLink.

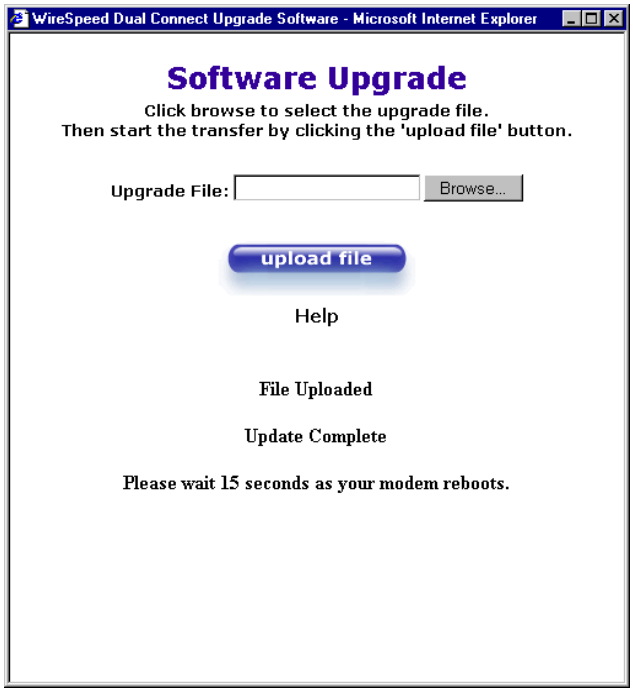


The screens below show that the file upload has completed and that the Programming Flash is being erased to prepare the Flash storage area for upload of the new file. (Programming Flash is a temporary storage area for uploaded files.)

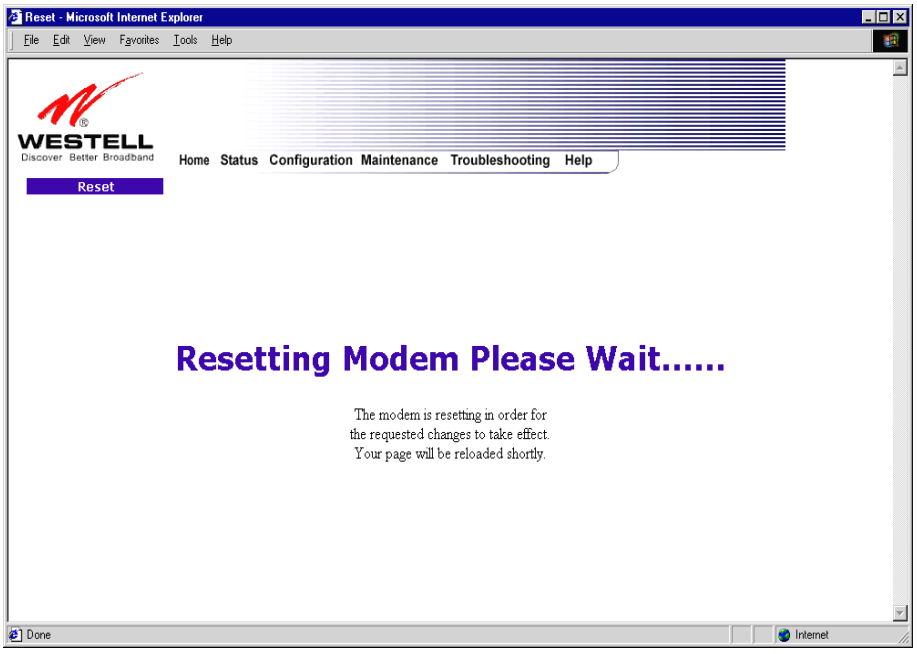




The screen below shows that the upload was successful. VersaLink will now reboot.


WireSpeed Dual Connect Upgrade Software - Microsoft Internet Explorer
Software Upgrade
Click browse to select the upgrade file.
Then start the transfer by clicking the 'upload file' button.
Upgrade File:
Browse...
upload file
Help
File Uploaded
Update Complete
Please wait 15 seconds as your modem reboots.

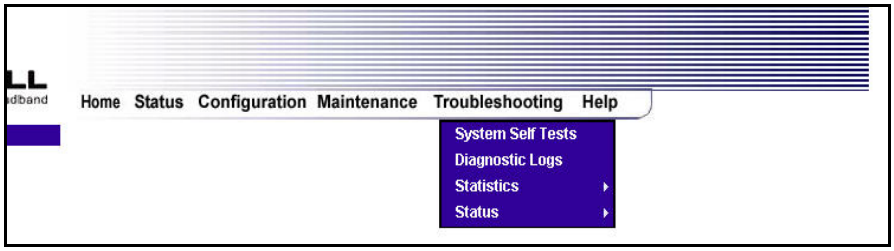
The following screen will be displayed as VersaLink is being reset.



After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that the PPP Status displays **UP.** (If necessary, click the **connect** button to establish your PPP session.)

16. TROUBLESHOOTING

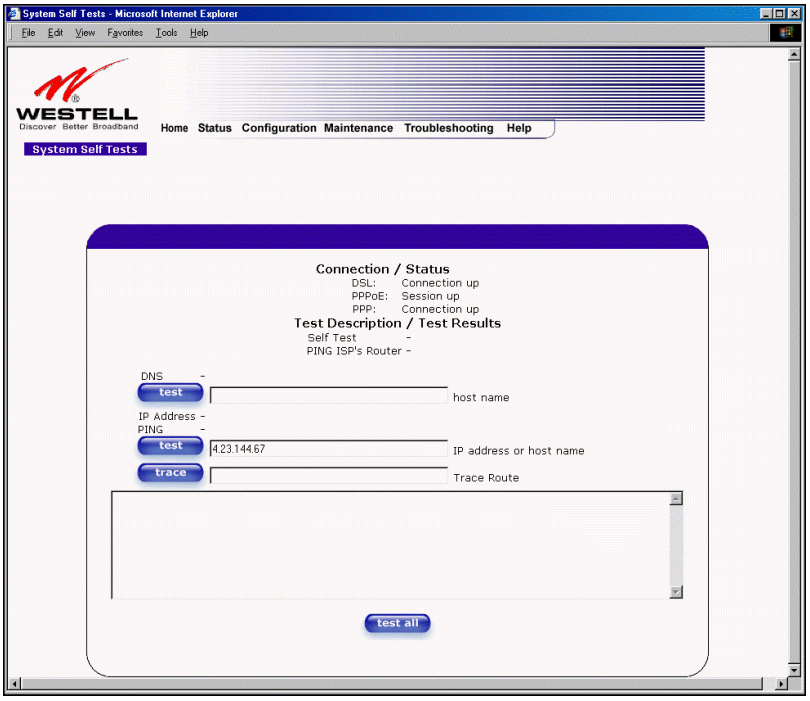
NOTE: Options in the **Troubleshooting** menu may or may not be displayed depending on VersaLinks WAN Configuration (DSLATM PORT or ETHERNET PORT 1). However, all menu options are displayed if VersaLink is configured for DSLATM PORT 1. The following sections provide further details on the Troubleshooting menu.



16.1 System Self Tests

The following screen will be displayed if you select **System Self Tests** from the **Troubleshooting** menu.

- To run a DNS test, type the appropriate host name in the field provided, and then click **Test.**
- To run a PING test, type the appropriate IP address or host name in the field provided, and then click **Test.**
- To run a Trace Route, type the appropriate IP address or host name in the field provided, and then click **Trace.**
- To run a full diagnostic test on your Gateway, click **Test All.**



If you want to PING using the System Self Test screen (diagnostics page) shown above, enter your **DNS** or **IP** address in the fields provided and click on the **test** button. The System Self Test will run a diagnostic test that executes independent of firewall security settings. See the following table for test descriptions and possible responses.

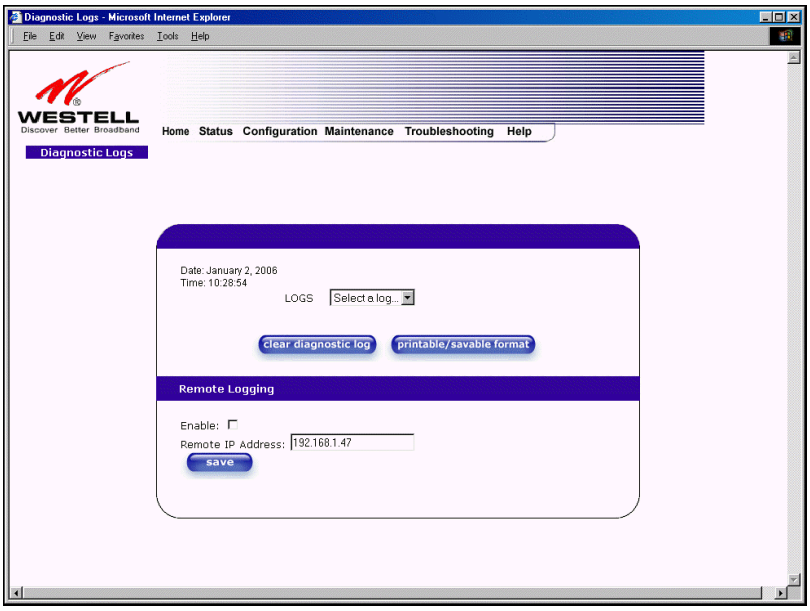
If you want to PING using the MS-DOS (shell) window, first you will need to check your firewall security setting. (If you PING via DOS shell you are susceptible to firewall rules, as this PING is dependent on VersaLink's firewall settings.) If your firewall is set to **Medium** or **High**, you will not be able to PING. You must set your firewall security setting to **Low** or **None**.

Connection/Status	
DSL	VersaLink checks the status of the DSL connection. Possible responses are: UP: VersaLink is operating correctly and has obtained synchronization with the opposing network device. DOWN: VersaLink is operating correctly, but has not synchronized with the opposing device.
PPPoE	Indicates that a PPPoE session is or is not established. Possible responses are: Session UP: A valid PPPoE session has been detected. No Session: Currently there is no active PPPoE session established. Initiating Session: A PPP session must be connected from the homepage screen.
PPP	Indicates that a PPPoE or PPPoA session must already be established. Possible responses are: Connection UP: VersaLink has established a connection No Connection: There is no PPP connection Initiating Connection: The PPP connection process has been initiated Connection Halted: A successful PPP connection was halted Cannot Connect: A PPP connection could not be made because of a PPPoE session failure. Authorization Failure: The user name or password is incorrect. Link Control Protocol Failed: Re-establish the session (from the home page).
Test Description / Test Results	
Self Test	Performs an integrity check of certain internal components of VersaLink.
PING ISP's VersaLink	Performs an IP network check (i.e., an IP Ping) of the Service Provider's VersaLink. This test verifies that VersaLink can exchange IP traffic with an entity on the other side of the DSL line. Possible responses are: Success: VersaLink has detected an IP Remote VersaLink connection. No Response: The IP Remote VersaLink does not answer the IP Ping. Could not test: The test could not be executed due to VersaLink settings. Check your DSL sync or your PPP session. You must have both a DSL sync and a PPP connection established to execute a PING.
DNS	Performs a test to try to resolve the name of a particular host. The host name is entered in the input box. Possible responses are: Success: VersaLink has successfully obtained the resolved address. The IP address is shown below the host name input box. No Response: VersaLink has failed to obtain the resolved address. Host not found: The DNS Server was unable to find an address for the given host name. No data, enter host name: No host name is specified. Could not test: The test could not be executed due to VersaLink settings. Check your DSL sync or your PPP session. You must have both a DSL sync and a PPP connection established to execute a PING.
IP Address	IP Address of the Host Name.
PING (via IP Address or Host Name)	Performs an IP connectivity check to a remote computer either within or beyond the service provider's network. You can PING a remote computer via the IP address or the DNS address. If your PING fails, try a different IP or DNS address. Possible responses are: Success: The Remote Host computer was detected. No Response: There was no response to the Ping from the remote computer. No name or address to PING: No host name or IP address was specified.

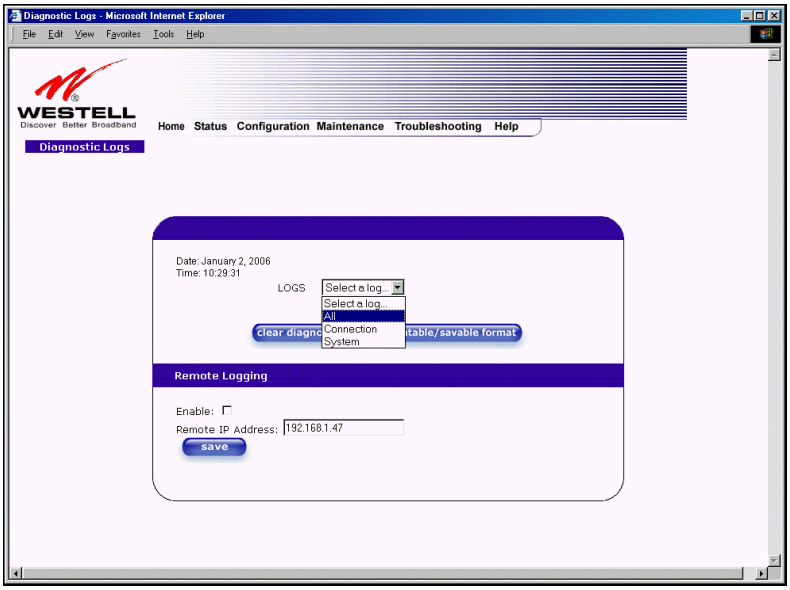
	Could not test: The test could not be executed due to VersaLink settings. Check your DSL sync or your PPP session. You must have both a DSL sync and a PPP connection established to execute a PING.
Trace	Determines the route taken to destination by sending Internet Control Message Protocol (ICMP) echo packets with varying IP Time-To-Live (TTL) values to the destination. Trace Route is used to determine where the packet is stopped on the network.

16.2 Diagnostic Logs

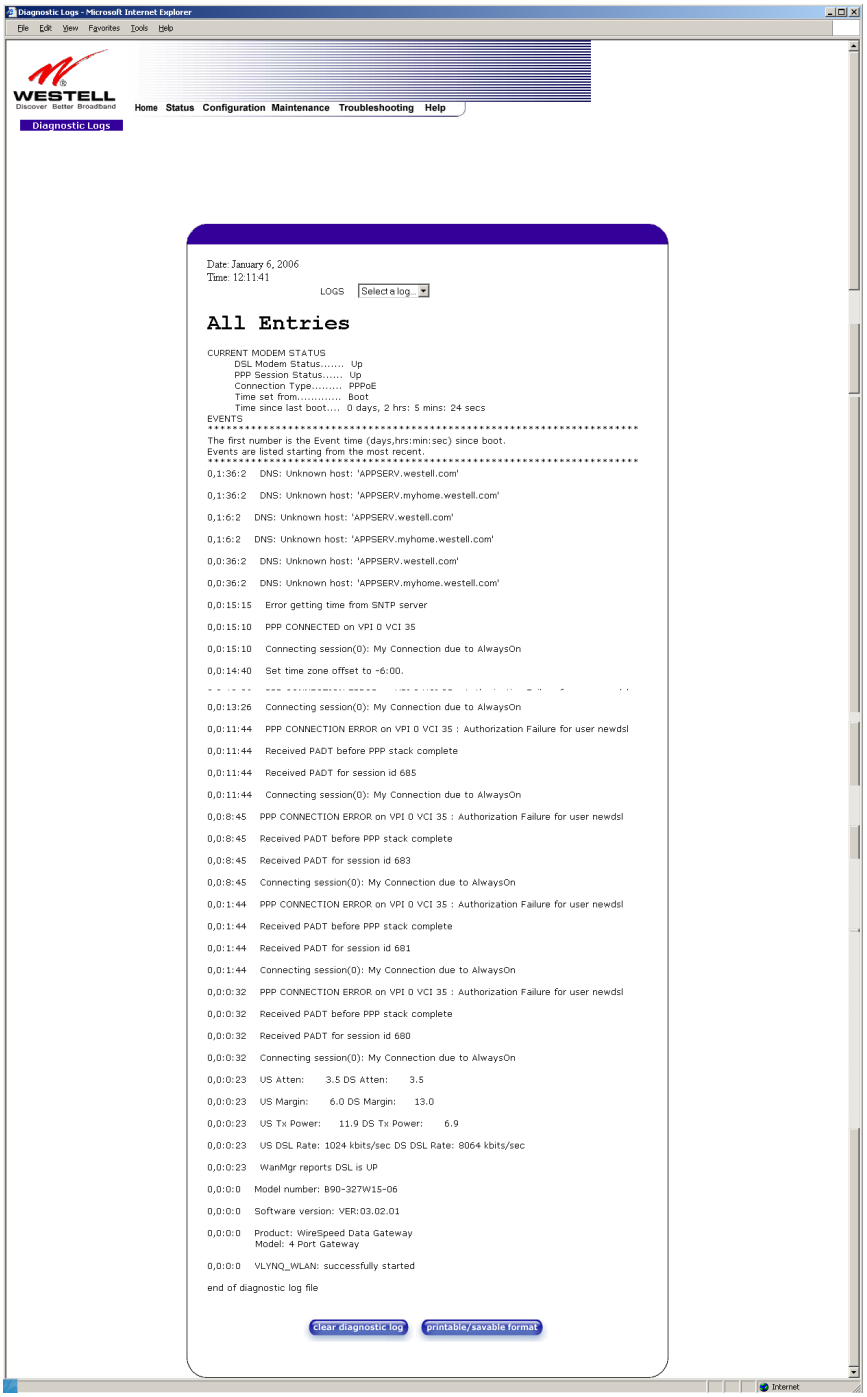
If you select **Diagnostic Logs**, from the **Troubleshooting** menu, the following screen will be displayed.



To view a diagnostic log, select an option from the **LOGS** drop-down menu.

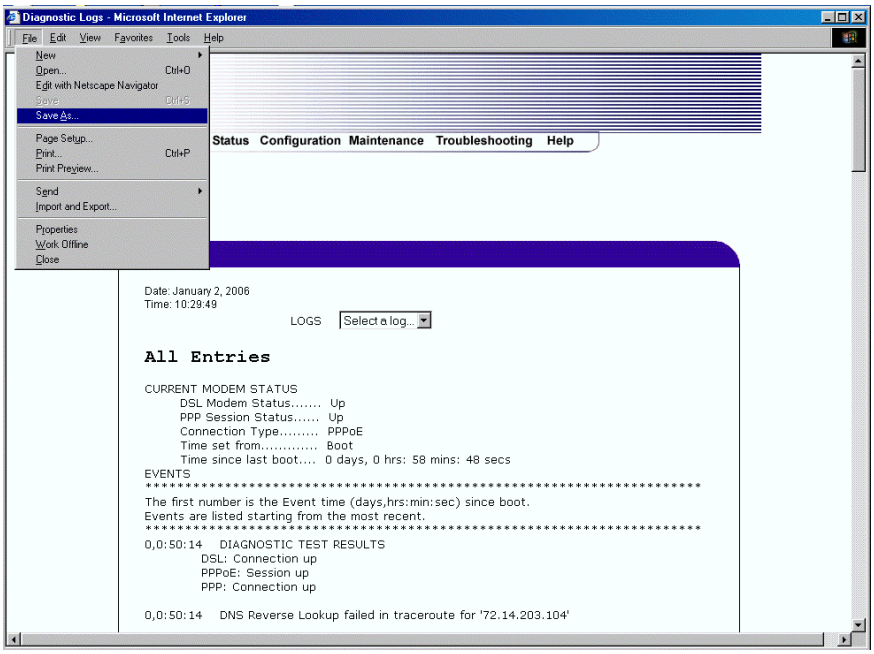


If you selected **All,** the following screen will be displayed. This screen provides a detailed list of VersaLink's connection status and system information. Click **clear diagnostic log** to clear the diagnostic log information.

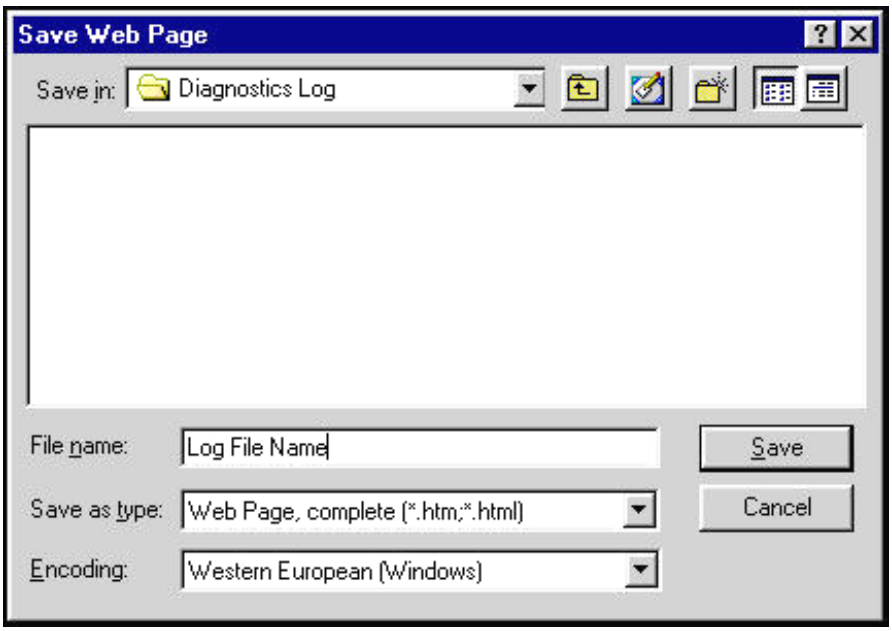

Diagnostic Logs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Diagnostic Logs
Date: January 6, 2006
Time: 12:11:41
LOGS Select a log...
All Entries
CURRENT MODEM STATUS
DSL Modem Status..... Up
PPP Session Status..... Up
Connection Type..... PPPoE
Time set from..... Boot
Time since last boot.... 0 days, 2 hrs: 5 mins: 24 secs
EVENTS
The first number is the Event time (days,hrs:min:sec) since boot.
Events are listed starting from the most recent.
0,1:36:2 DNS: Unknown host: 'APPSERV.westell.com'
0,1:36:2 DNS: Unknown host: 'APPSERV.myhome.westell.com'
0,1:6:2 DNS: Unknown host: 'APPSERV.westell.com'
0,1:6:2 DNS: Unknown host: 'APPSERV.myhome.westell.com'
0,0:36:2 DNS: Unknown host: 'APPSERV.westell.com'
0,0:36:2 DNS: Unknown host: 'APPSERV.myhome.westell.com'
0,0:15:15 Error getting time from SNTP server
0,0:15:10 PPP CONNECTED on VPI 0 VCI 35
0,0:15:10 Connecting session(0): My Connection due to AlwaysOn
0,0:14:40 Set time zone offset to -6:00.
0,0:13:26 Connecting session(0): My Connection due to AlwaysOn
0,0:11:44 PPP CONNECTION ERROR on VPI 0 VCI 35 : Authorization Failure for user newdsl
0,0:11:44 Received PADT before PPP stack complete
0,0:11:44 Received PADT for session id 685
0,0:11:44 Connecting session(0): My Connection due to AlwaysOn
0,0:8:45 PPP CONNECTION ERROR on VPI 0 VCI 35 : Authorization Failure for user newdsl
0,0:8:45 Received PADT before PPP stack complete
0,0:8:45 Received PADT for session id 683
0,0:8:45 Connecting session(0): My Connection due to AlwaysOn
0,0:1:44 PPP CONNECTION ERROR on VPI 0 VCI 35 : Authorization Failure for user newdsl
0,0:1:44 Received PADT before PPP stack complete
0,0:1:44 Received PADT for session id 681
0,0:1:44 Connecting session(0): My Connection due to AlwaysOn
0,0:0:32 PPP CONNECTION ERROR on VPI 0 VCI 35 : Authorization Failure for user newdsl
0,0:0:32 Received PADT before PPP stack complete
0,0:0:32 Received PADT for session id 680
0,0:0:32 Connecting session(0): My Connection due to AlwaysOn
0,0:0:23 US Atten: 3.5 DS Atten: 3.5
0,0:0:23 US Margin: 6.0 DS Margin: 13.0
0,0:0:23 US Tx Power: 11.9 DS Tx Power: 6.9
0,0:0:23 US DSL Rate: 1024 kbits/sec DS DSL Rate: 8064 kbits/sec
0,0:0:23 WanMgr reports DSL is UP
0,0:0:0 Model number: B90-327W15-06
0,0:0:0 Software version: VER:03.02.01
0,0:0:0 Product: WireSpeed Data Gateway
Model: 4 Port Gateway
0,0:0:0 VLYNQ_WLAN: successfully started
end of diagnostic log file
clear diagnostic log
printable/savable format
Internet

16.2.1 Saving the Diagnostic Log File

To save a diagnostic log file, go to your Browser's menu and select **File > Save As**.

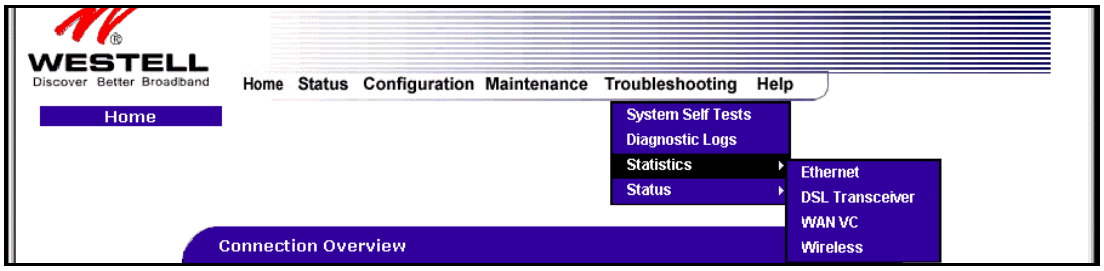


At the **Save Web Page** dialog box, select a destination for your log file from the **Save in** drop-down menu. Next, enter a name for your log file in the field labeled **File name,** and then click **Save** to save the log file.



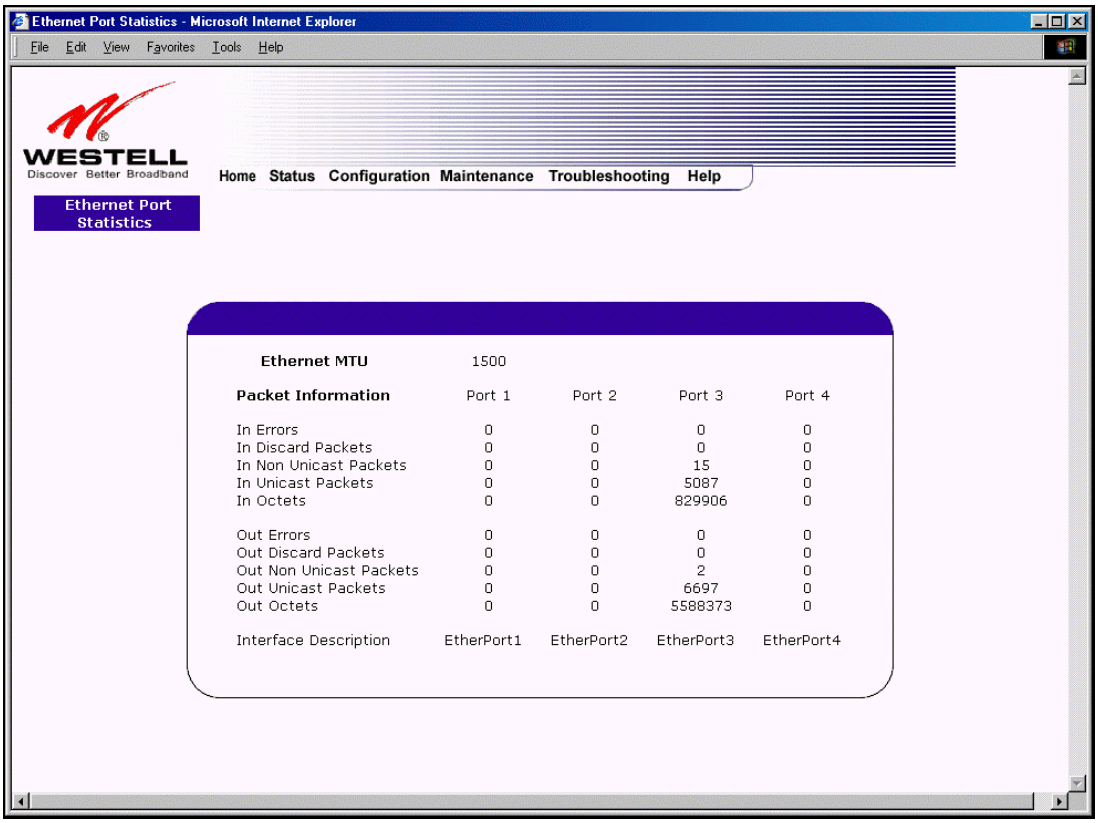
16.3 Statistics

NOTE: If VersaLink is configured for **ETHERNET PORT 1**, only **Ethernet** and **Wireless** statistics will be displayed in the **Statistics** menu. The **DSL Transceiver** statistics and the **WAN VC** statistics will not be displayed. If you want to view **DSL Transceiver** and **WAN VC** statistics, you must configure VersaLink for **DSLATM PORT.** Refer to section 13.6.2.2 for additional details.



16.3.1 Ethernet Port Statistics

The following screen will be displayed if you select **Statistics > Ethernet** from the **Troubleshooting** menu.

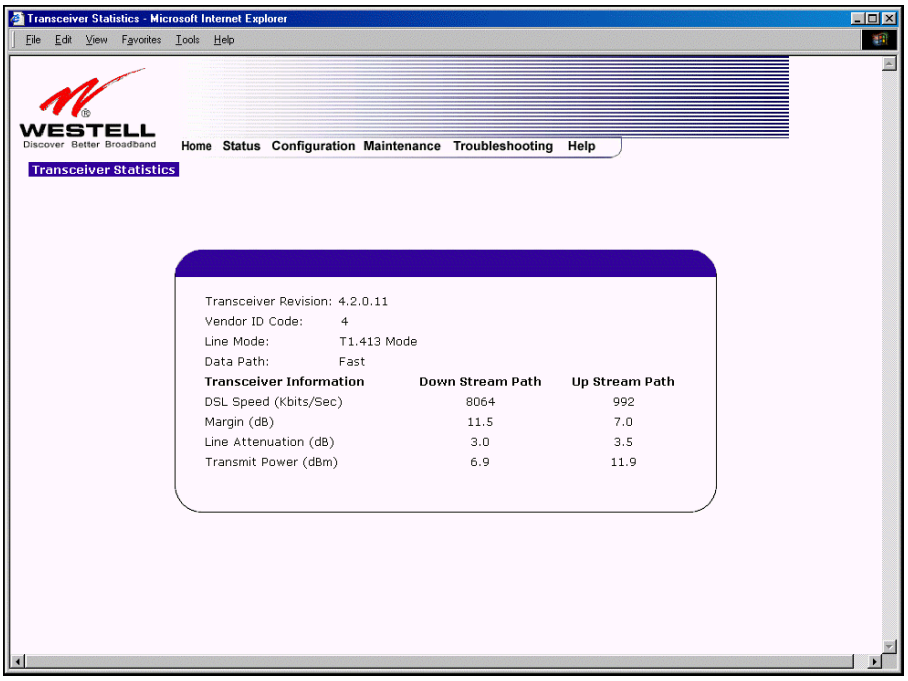

Ethernet Port Statistics - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Ethernet Port Statistics
Ethernet MTU 1500
Packet Information Port 1 Port 2 Port 3 Port 4
In Errors 0 0 0 0
In Discard Packets 0 0 0 0
In Non Unicast Packets 0 0 15 0
In Unicast Packets 0 0 5087 0
In Octets 0 0 829906 0
Out Errors 0 0 0 0
Out Discard Packets 0 0 0 0
Out Non Unicast Packets 0 0 2 0
Out Unicast Packets 0 0 6697 0
Out Octets 0 0 5588373 0
Interface Description EtherPort1 EtherPort2 EtherPort3 EtherPort4

In Errors	The number of error packets received on the Ethernet interface.
In Discard Packets	The number of discarded packets received.
In Non Unicast Packets	The number of non-Unicast packets received on the Ethernet interface.
In Unicast Packets	The number of Unicast packets received on the Ethernet interface.
In Octets	The number of bytes received on the Ethernet interface.
Out Errors	The number of outbound packets that could not be transmitted due to errors.
Out Discard Packets	The number of outbound packets discarded.
Out Non Unicast Packets	The number of non-Unicast packets transmitted on the Ethernet interface.
Out Unicast Packets	The number of Unicast packets transmitted on the Ethernet interface.
Out Octets	The number of bytes transmitted on the Ethernet interface.
MTU	Maximum Transmission Unit- The number of data bytes contained in the Ethernet frame.
Interface Type	A unique identifier that represents the interface type.
Interface Description	A description field that refers to the interface type.

16.3.2 DSL Transceiver Statistics

The following screen will be displayed if you select **Statistics > DSL Transceiver** from the **Troubleshooting** menu.

NOTE: If VersaLink is configured using **ETHERNET PORT 1**, the following screen will not be available.


Transceiver Statistics - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Transceiver Statistics
Transceiver Revision: 4.2.0.11
Vendor ID Code: 4
Line Mode: T1.413 Mode
Data Path: Fast
Transceiver Information Down Stream Path Up Stream Path
DSL Speed (Kbits/Sec) 8064 992
Margin (dB) 11.5 7.0
Line Attenuation (dB) 3.0 3.5
Transmit Power (dBm) 6.9 11.9

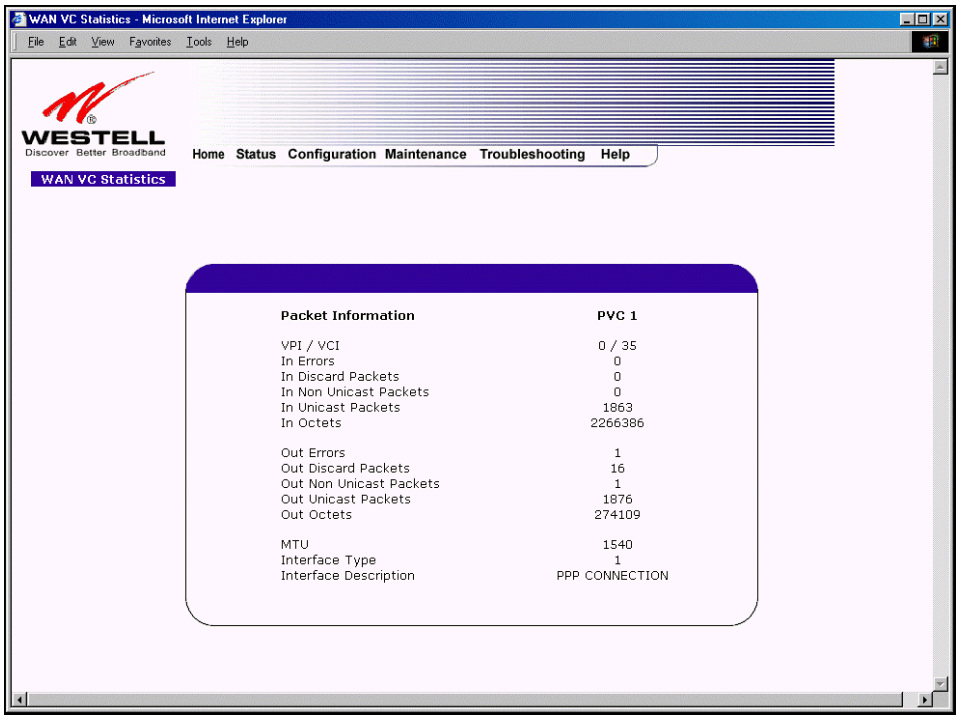
Transceiver Revision	The transceiver software version number.
Vendor ID Code	The CPE Vendor's ID code for their chipset.
Line Mode	The operational mode. Modes supported are No Mode, Multi Mode, T.1413 Mode, G.DMT Mode, and G.LITE Mode.
Data Path	The data path used (either Fast or Interleaved).
Transceiver Information-Down Stream/Up Stream Path	
DSL Speed (Kbits/Sec)	The transmission rate that is provided by your ISP.
SNR Margin (db)	The Signal-to-Noise Ratio (S/N) where 0 db = $1x10^{-7}$, which inhibits your DSL

	speed.
Line Attenuation (dB)	The DSL line loss.
Transmit Power (db/Hz)	The transmitted signal strength.

16.3.3 WAN VC Statistics

The following screen will be displayed if you select **Statistics > WAN VC** from the **Troubleshooting** menu.

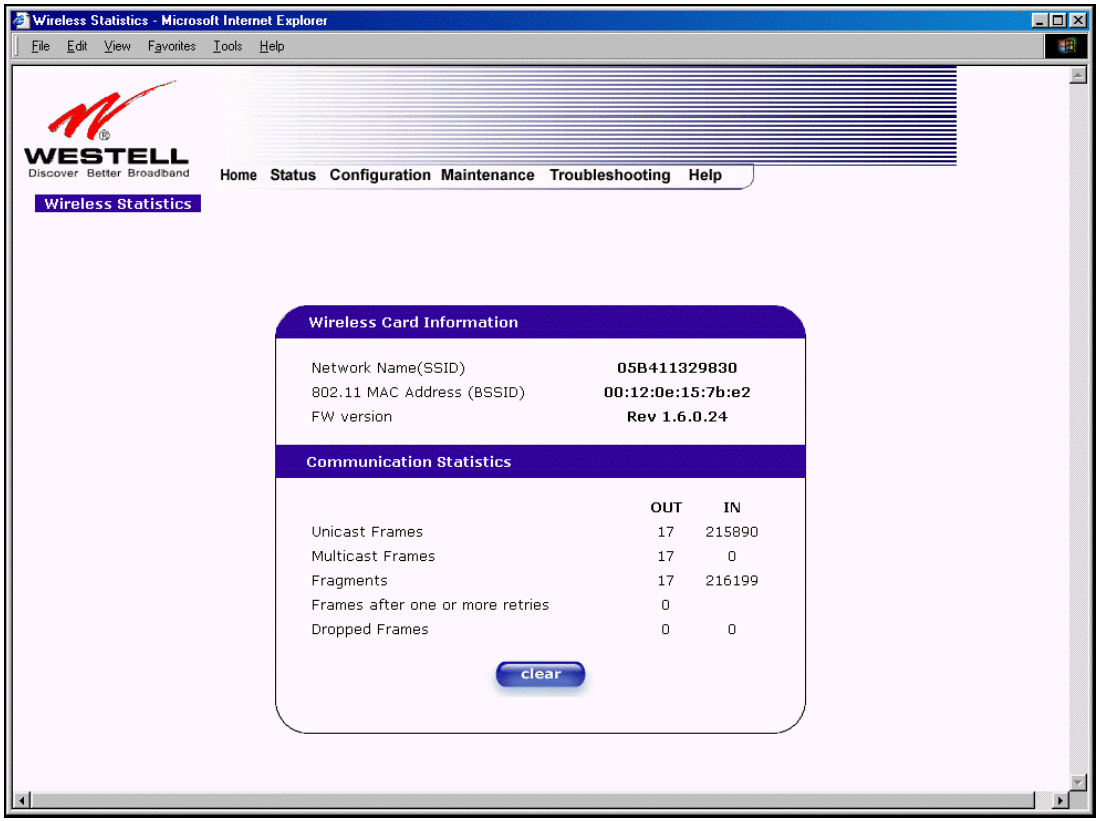
NOTE: If VersaLink is configured using **ETHERNET PORT 1**, the following screen will not be available.


WAN VC Statistics - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
WAN VC Statistics
Packet Information PVC 1
VPI / VCI 0 / 35
In Errors 0
In Discard Packets 0
In Non Unicast Packets 0
In Unicast Packets 1863
In Octets 2266386
Out Errors 1
Out Discard Packets 16
Out Non Unicast Packets 1
Out Unicast Packets 1876
Out Octets 274109
MTU 1540
Interface Type 1
Interface Description PPP CONNECTION

VPI/VCI	Displays the VPI/VCI values obtained from your ISP.
In Errors	The number of error packets received on the ATM port.
In Discard Packets	The number of discarded packets received.
In Non Unicast Packets	The number of non-Unicast packets received on the ATM port.
In Unicast Packets	The number of Unicast packets received on the ATM port.
In Octets	The number of bytes received on the ATM port.
Out Errors	The number of outbound packets that could not be transmitted due to errors.
Out Discard Packets	The number of outbound packets discarded.
Out Non Unicast Packets	The number of non-Unicast packets transmitted on the ATM port.
Out Unicast Packets	The number of Unicast packets transmitted on the ATM port.
Out Octets	The number of bytes transmitted on the ATM port.
MTU	Maximum Transmission Unit -The number of data bytes contained in an ATM frame.
Interface Type	A unique identifier that represents the interface type.
Interface Description	A description field that refers to the interface type.

16.4 Wireless Statistics

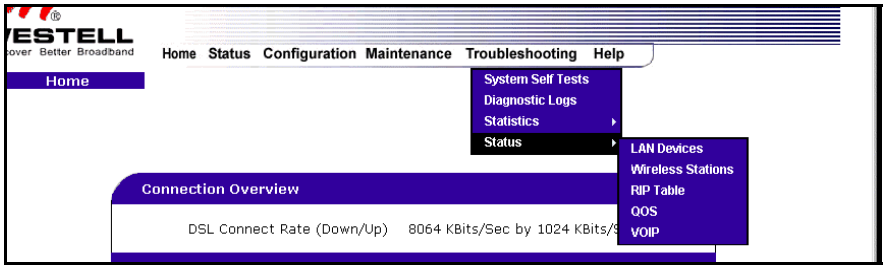
The following screen will be displayed if you select **Statistics > Wireless** from the **Troubleshooting** menu.



Wireless Card Information	
Network Name (SSID)	This string, (32 characters or less) is the name associated with the Access Point (AP). To connect to the AP, the Service Set ID (SSID) on a Station card must match the SSID on the AP.
802.11 MAC Address (BSSID)	This is the Media Access Controller address of the AP. It is used as the Basic Service Set Identifier (BSSID).
FW Version	This is the Network Interface Card Identifier. It uniquely identifies the hardware platform of the AP. This is used with other information to determine if the inserted card can be used as an AP, and if so, the version of AP firmware to be used. Not all makes of wireless station cards can be used as an AP.
Communication Statistics	
NOTE: Data preceded by **OUT** pertain to transmissions from the VersaLink to a station; VersaLink is the source. Data preceded by **IN** pertain to data received by VersaLink; VersaLink is the destination.	
OUT-Unicast Frames	The number of successfully transmitted frames whose destination address was a single station; not necessarily the same station, but to any single station as opposed to a transmission that multiple stations would receive-as in the case of broadcast message.
OUT-Multicast Frames	The number of successfully transmitted frames whose destination address was a multicast address (received by more that one station): not necessarily broadcast to all stations, but more than a single station. Broadcast messages are included in the count.
OUT-Fragments	The number of successful transmissions made. This will typically be greater than the sum of the Unicast and Multicast frames because large

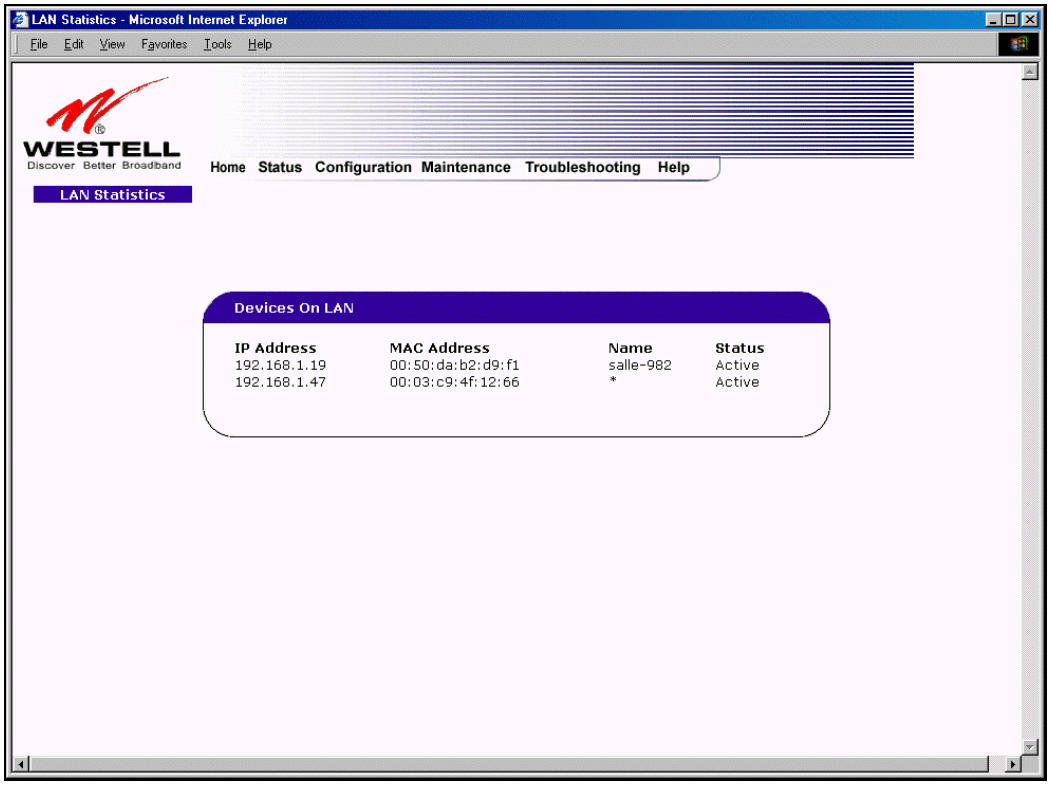
	frames are broken into multiple transmissions. The number of fragments per frame is based on the Fragmentation Threshold setting (not user-configurable).
OUT-Frames after one or more retries	The number of frames that successfully transmitted after more than one retry. Any fragment of a frame that required multiple retries would increment this counter for the whole frame.
OUT-Dropped Frames, too many retries	The number of frames that did not transmit due to the short or long retry limit being reached because no acknowledgement or CTS was received.
IN-Unicast Frames	The number of successfully received frames whose destination address was a single location, not necessarily the same location, but to any single location as opposed to the broadcast address.
IN-Multicast Frames	The number of successfully received frames whose destination address was a multicast address. Broadcast messages are included in this count.
IN-Fragments	The number of fragments successfully received. This may not be equal to the sum of the Unicast and Multicast frames because large frames are broken into multiple transmissions. The number of fragments per frame is based on the Fragmentation Threshold setting (not user-configurable) on the source station.
IN-Frames after one or more retries	The number of frames that successfully transmitted after more than one retry. Any fragment of a frame that required multiple retries would increment this counter for the whole frame.
IN-Drops due to insufficient Rx buffers	The number of received frames discarded due to lack of buffer space.

16.5 Status



16.5.1 LAN Devices

The following screen will be displayed if you select **Status > LAN Devices** from the **Troubleshooting** menu.

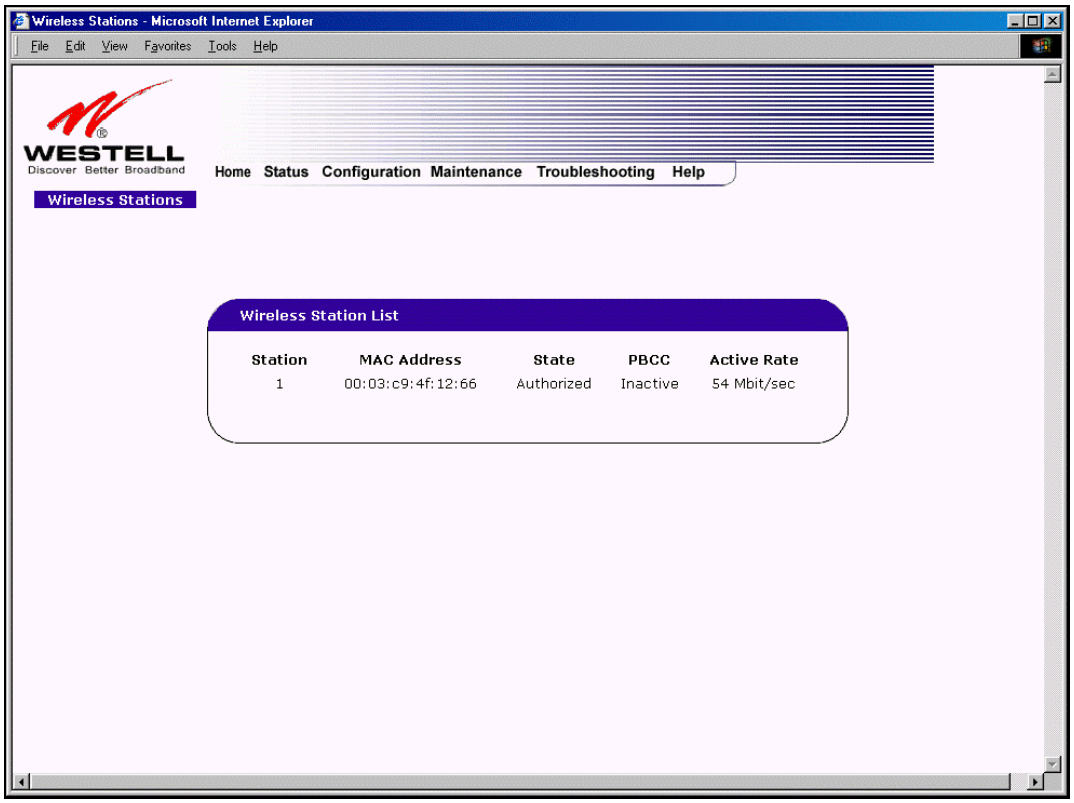

LAN Statistics - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
LAN Statistics
Devices On LAN
IP Address MAC Address Name Status
192.168.1.19 00:50:da:b2:d9:f1 salle-982 Active
192.168.1.47 00:03:c9:4f:12:66 * Active

Devices on LAN	
IP Address	Displays the IP network address that VersaLink is on.
MAC Address	Media Access Controller (MAC) address of this device.
Name	Displays the ASCII (text) name of the devices connected to the LAN.
Status	Displays the status of the devices connected to the LAN.

16.5.2 Wireless Stations

The following screen will be displayed if you select **Status > Wireless** from the **Troubleshooting** menu.

NOTE: A Wireless device must be connected to the Gateway for this table to be populated.

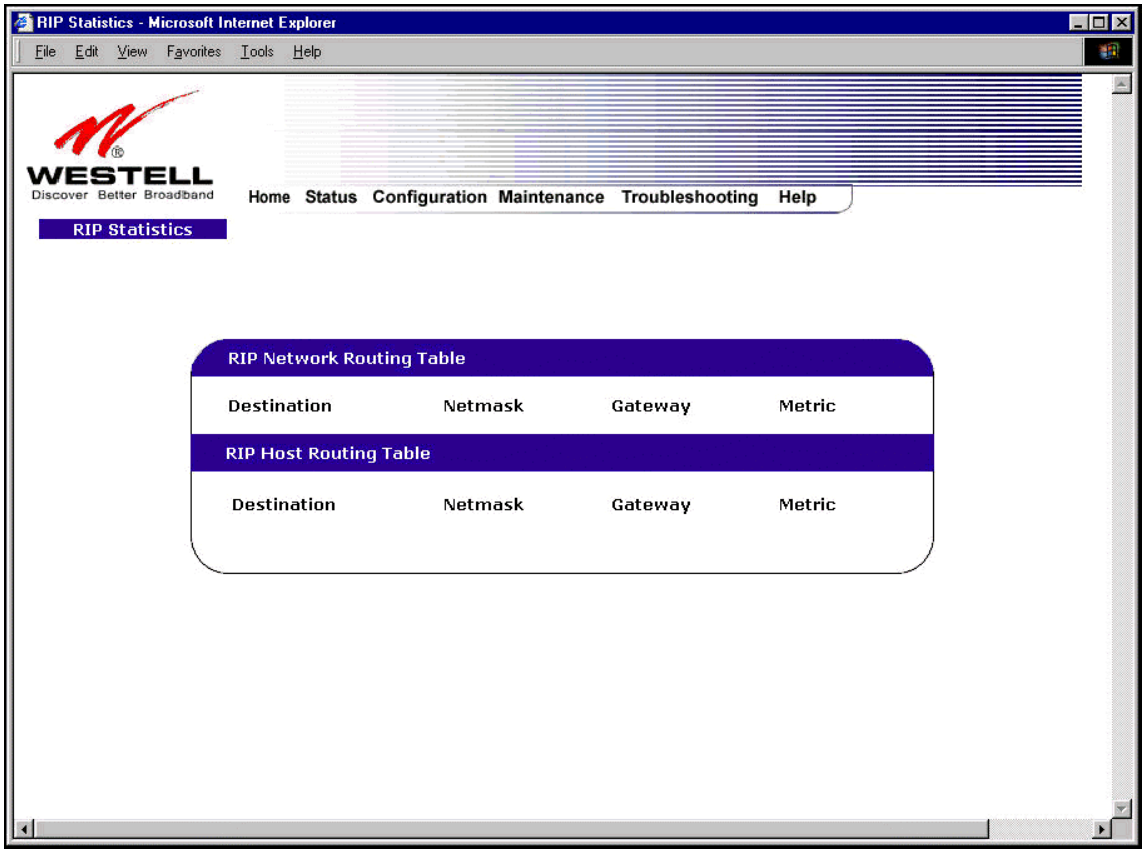

Wireless Stations - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
Wireless Stations
Wireless Station List
Station MAC Address State PBCC Active Rate
1 00:03:c9:4f:12:66 Authorized Inactive 54 Mbit/sec

Wireless Stations List	
Station	This number indicates the order in which the stations are first accessed by VersaLink.
MAC Address	The Media Access Controller Address assigned to the station.
State	The current state of the negotiation between the station and VersaLink.
PBCC	Indicates whether the station that is associated with VersaLink operates in PBCC (Packet Binary Convolutional Code) modulation.
Active Rate	The current transmit and receive rate.

16.5.3 RIP Table

The following screen will be displayed if you select **Status > RIP Table** from the **Troubleshooting** menu.

NOTE: RIP must be enabled for this table to be populated.


RIP Statistics - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
RIP Statistics
RIP Network Routing Table
Destination Netmask Gateway Metric
RIP Host Routing Table
Destination Netmask Gateway Metric

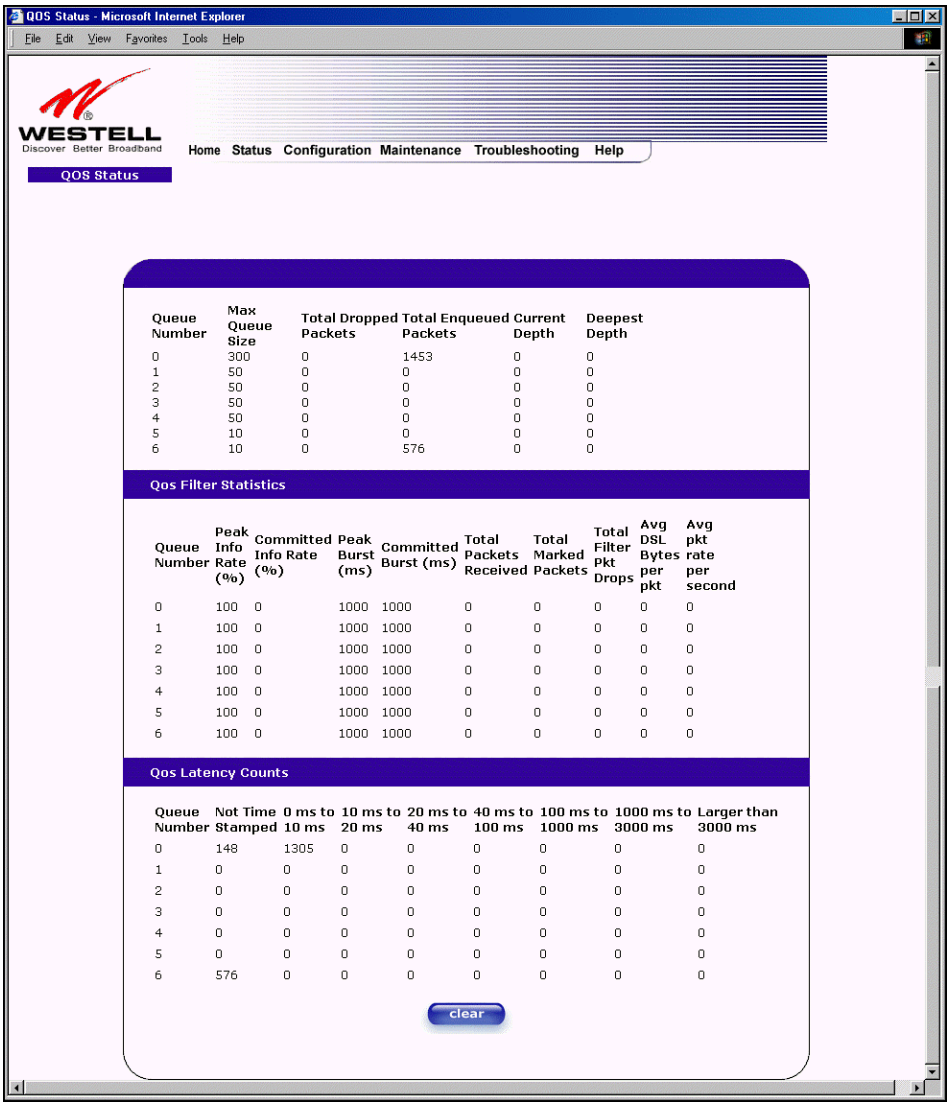
RIP Network Routing Table	Indicates Network routes received via RIP.
RIP Host Routing Table	The Host routes received via RIP.
Destination	The destination IP address of the route
Netmask	The IP mask of the route
Gateway	The gateway of the route
Metric	The RIP metric (0-15). A lower value is better.

16.5.4 QOS Status

The following screen will be displayed if you select **Status > QOS** from the **Troubleshooting** menu.

NOTE: If VersaLink is configured using **ETHERNET PORT 1**, the following screen will not be available.

Click the **clear** button to clear all counts and statistics (not just latency counts). This does not affect the configuration values. QoS must be enabled on the Gateway for this table to be populated.

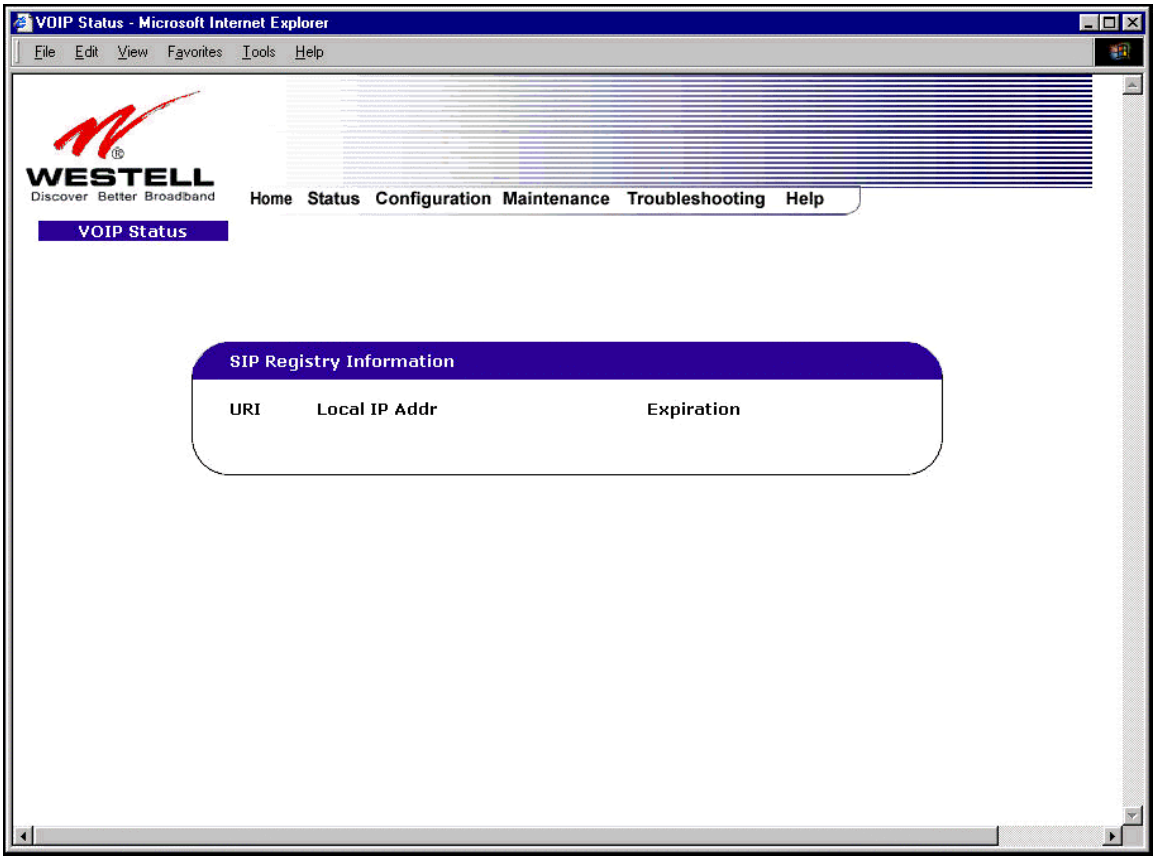

QOS Status - Microsoft Internet Explorer
File Edit View Favorites Tools Help
WESTELL
Discover Better Broadband
Home Status Configuration Maintenance Troubleshooting Help
QOS Status
Queue Number
Max Queue Size
Total Dropped Packets
Total Enqueued Packets
Current Depth
Deepest Depth
0 300 0 1453 0 0
1 50 0 0 0 0
2 50 0 0 0 0
3 50 0 0 0 0
4 50 0 0 0 0
5 10 0 0 0 0
6 10 0 576 0 0
Qos Filter Statistics
Queue Number
Peak Info Rate (%)
Committed Info Rate (%)
Peak Burst (ms)
Committed Burst (ms)
Total Packets Received
Total Marked Packets
Total Filter Pkt Drops
Avg DSL Bytes per pkt
Avg pkt rate per second
0 100 0 1000 1000 0 0 0 0 0
1 100 0 1000 1000 0 0 0 0 0
2 100 0 1000 1000 0 0 0 0 0
3 100 0 1000 1000 0 0 0 0 0
4 100 0 1000 1000 0 0 0 0 0
5 100 0 1000 1000 0 0 0 0 0
6 100 0 1000 1000 0 0 0 0 0
Qos Latency Counts
Queue Number
Not Time Stamped
0 ms to 10 ms
10 ms to 20 ms
20 ms to 40 ms
40 ms to 100 ms
100 ms to 1000 ms
1000 ms to 3000 ms
Larger than 3000 ms
0 148 1305 0 0 0 0 0 0
1 0 0 0 0 0 0 0 0
2 0 0 0 0 0 0 0 0
3 0 0 0 0 0 0 0 0
4 0 0 0 0 0 0 0 0
5 0 0 0 0 0 0 0 0
6 576 0 0 0 0 0 0 0
clear

Queue Number	Indicates the DiffServ Queue. Possible responses are: 0 = Best Effort (BE) 1 = Assured Forwarding 1 (AF1) 2 = Assured Forwarding 2 (AF2) 3 = Assured Forwarding 2 (AF3) 4 = Assured Forwarding 2 (AF4) 5 = Expedited Forwarding (EF) 6 = Routing Protocols (DiffServ priorities 6 and 7)
Max Queue Size	The maximum number of packets that can be queued for this priority.
Total Dropped Packets	Indicates how many packets of this priority have been dropped by QOS due to lack of buffer space or filtering rules.
Total Enqueued Packets	Displays the number of packets, destined for the WAN, that have been received.
Current Depth	Displays the current number of packets of this priority that are queued.
Deepest Depth	Displays the most number of packets that have been queued at once for this priority.
QOS Filter Statistics	
Queue Number	The DiffServ Queue. (See Queue Number description above.)
Peak Info. Rate (%)	The maximum allowed rate for this priority, expressed as a percentage of the DSL rate.
Committed Info Rate (%)	The committed rate for this priority, expressed as a percentage of the DSL rate
Peak Burst (ms)	Displays the interval in milliseconds for averaging the peak offered rate.
Committed Burst (ms)	Displays the interval in milliseconds for averaging the committed offered rate.
Total Packets Received	Displays the total number of packets of this priority that are destined for the LAN.
Total Marked Packets	Displays the number of packets of this priority that exceeded the committed rate, but not the peak rate, and were marked with a higher drop priority
Total Filter Packet Drops	Displays the number of packets of this priority that exceeded the peak rate and that were, therefore, dropped.
Avg. DSL Bytes Per Packet	Displays the average size of packets for this priority, including all overhead.
Avg. Packet Rate Per second	Displays the average rate (in packets per seconds) for this priority.
QOS Latency Counts	
Queue Number	The DiffServ Queue. (See Queue Number description above.)
Not Time Stamped	The packets with no incoming time stamp. (Often these are generated internal to the modem.)
A ms to B ms	The number of packets of this priority whose time in the modem fell between A and B milliseconds. (Time is measured from the point the packet arrives at the modem's processor until is passed to the ATM hardware for transmission.) Possible ranges are (A ms to B ms): 0 ms to 10 ms 10 ms to 20 ms 20 ms to 40 ms 40 ms to 100 ms 100 ms to 1000 ms 1000 ms to 3000 ms Larger than 3000 ms

16.5.5 VOIP Status

The following screen will be displayed if you select **Status > VOIP** from the **Troubleshooting** menu.

NOTE: A VOIP device must be connected to the Gateway for this table to be populated.



SIP Registry Information	
URI	The SIP URI that is trying to register. (This field only indicates that a SIP device tried to register, not that it succeeded.)
Local IP Address	The local, LAN IP address of the SIP device.
Expiration	Indicates how long (in seconds) until the registration expires.

17. NAT SERVICES

For your convenience, VersaLink supports protocols for Applications, Games, and VPN-specific programs. The following chart provides protocol information for the services supported by VersaLink.

NOTE: To configure VersaLink for a service or application, follow the steps in section 14 (Setting Up Advanced Service Configuration) of this User Guide.

Applications/Games/VPN Support

Application/Game	Port/Protocol
Aliens vs. Predator	80 UDP, 2300 UDP, 8000-8999 UDP
America Online	5190 TCP/UDP
AoE II: Conquors	47624 TCP/UDP, 6073 TCP/UDP, 2300-2400 TCP/UDP
AOL Instant Messenger	4099 TCP, 5190 TCP
Asheron's Call	9000-9013 UDP, 28800-29000 TCP
Battlecom	2300-2400 TCP/UDP, 47624 TCP/UDP
Black and White	2611-2612 TCP, 6667 TCP, 6500 UDP, 27900 UDP
Blizzard Battle.net (Diablo II)	4000 TCP, 6112 TCP/UDP
Buddy Phone	700, 701 UDP
Bungie.net, Myth, Myth II Server	3453 TCP
Calista IP Phone	3000 UDP, 5190 TCP
Citrix Metaframe	1494 TCP
Client POP/IMAP	110 TCP
Client SMTP	25 TCP
Counter Strike	27015 TCP/UDP, 27016 TCP/UDP
Dark Reign 2	26214 TCP/UDP
Delta Force (Client and Server)	3568 UDP, 3100-3999 TCP/UDP
Delta Force 2	3568-3569 UDP
DeltaForce: Land Warrior	UDP 53 TCP 21 TCP 7430 TCP 80 UDP 1029 UDP 1144 UDP 65436 UDP 17478
DNS	53 UDP
Elite Force	2600 UDP, 27500 UDP, 27910 UDP, 27960 UDP
Everquest	1024-7000 TCP/UDP
F-16, Mig 29	3863 UDP
F-22 Lightning 3	4660-4670 TCP/UDP, 3875 UDP, 4533-4534 UDP, 4660-4670 UDP
F-22 Raptor	3874-3875 UDP
Fighter Ace II	50000-50100 TCP/UDP
Fighter Ace II for DX play	50000-50100 TCP/UDP, 47624 TCP, 2300-2400 TCP/UDP

Application/Game	Port/Protocol
FTP	20 TCP, 21 TCP
GameSpy Online	UDP 3783 UDP 6515 TCP 6667 UDP 12203 TCP/UDP 13139 UDP 27900 UDP 28900 UDP 29900 UDP 29901
Ghost Recon	TCP 80 UDP 1038 UDP 1032 UDP 53 UDP 2347 UDP 2346
GNUtella	6346 TCP/UDP, 1214 TCP
Half Life Server	27005 UDP(client only) 27015 UDP
Heretic II Server	28910 TCP
Hexen II	26900 (+1) each player needs their own port. Increment by one for each person
Hotline Server	5500, 5503 TCP 5499 UDP
HTTPS	443 TCP/UDP
ICMP Echo	4 ICMP
ICQ OLD	4000 UDP, 20000-20019 TCP
ICQ 2001b	4099 TCP, 5190 TCP
ICUII Client	2000-2038 TCP, 2050-2051 TCP, 2069 TCP, 2085 TCP, 3010-3030 TCP
ICUII Client Version 4.xx	1024-5000 TCP, 2050-2051 TCP, 2069 TCP, 2085 TCP, 3010-3030 TCP, 2000-2038 TCP6700-6702 TCP, 6880 TCP, 1200-16090 TCP
IMAP	119 TCP/UDP
IMAP v.3	220 TCP/UDP
Internet Phone	22555 UDP
IPSEC ESP	PROTOCOL 50
IPSEC IKE	500 UDP
Ivisit	9943 UDP, 56768 UDP
KALI, Doom & Doom II	2213 UDP, 6666 UDP (EACH PC USING KALI MUST USE A DIFFERENT PORT NUMBER STARTING WITH 2213 + 1
KaZaA	1214 TCP/UDP
Limewire	6346 TCP/UDP, 1214 TCP
Medal Of Honor: Allied Assault	TCP 80 UDP 53 UDP 2093 UDP 12201 TCP 12300 UDP 2135 UDP 2139 TCP/UDP 28900
mIRC Chat	6660-6669 TCP

Application/Game	Port/Protocol
Motorhead Server	16000 TCP/UDP, 16010-16030 TCP/UDP
MSN Game Zone	6667 TCP, 28800-29000 TCP
MSN Game Zone (DX 7 & 8 play)	6667 TCP, 6073 TCP, 28800-29000 TCP, 47624 TCP, 2300-2400 TCP/UDP
MSN Messenger	6891-6900 TCP, 1863 TCP/UDP, 5190 UDP, 6901 TCP/UDP
Napster	6699 TCP
Need for Speed 3, Hot Pursuit	1030 TCP
Need for Speed, Porsche	9442 UDP
Net2Phone	6801 UDP
NNTP	119 TCP/UDP
Operation FlashPoint	47624 UDP, 6073 UDP, 2300-2400 TCP/UDP, 2234 TCP
Outlaws	5310 TCP/UDP
Pal Talk	2090-2091 TCP/UDP, 2095 TCP, 5001 TCP, 8200-8700 TCP/UDP, 1025-2500 UDP
pcAnywhere host	5631 TCP, 5632 UDP, 22 UDP
Phone Free	1034-1035 TCP/UDP, 9900-9901 UDP, 2644 TCP, 8000 TCP
Quake 2	27910 UDP
Quake 3	27660 UDP Each computer playing QuakeIII must use a different port number, starting at 27660 and incrementing by 1. You'll also need to do the following: 1. Right click on the QIII icon 2. Choose "Properties" 3. In the Target field you'll see a line like "C:\Program Files\Quake III Arena\quake3.exe" 4. Add the Quake III net_port command to specify a unique communication port for each system. The complete field should look like this: "C:\Program Files\Quake III Arena\quake3.exe" +set net_port 27660 5. Click OK. 6. Repeat for each system behind the NAT, adding one to the net_port selected (27660,27661,27662)
Quicktime 4/Real Audio	6970-32000 UDP, 554 TCP/UDP
Rainbow Six & Rogue Spear	2346 TCP
RealOne Player	TCP - 554, 7070 to 7071 UDP - 6970 to 7170
Real Audio	6970-7170 UDP
Roger Wilco	TCP/UDP 3782 UDP 3783 (BaseStation)
ShoutCast Server	8000-8005 TCP
SSH Secure Shell	22 TCP/UDP
Starcraft	2346 TCP
Starfleet Command	2300-2400 TCP/UDP, 47624 TCP/UDP
Telnet	23 TCP
Tiberian Sun & Dune 2000	1140-1234, 4000 TCP/UDP
Ultima Online	5001-5010 TCP, 7775-7777 TCP, 8800-8900 TCP, 9999 UDP, 7875 UDP
Unreal Tournament server	7777 (default gameplay port) 7778 (server query port 7779,7779+ are allocated dynamically for each helper UdpLink objects,

Application/Game	Port/Protocol
	including UdpServerUplin objects. Try starting with 7779-7781 and add ports if needed 27900 server query, if master server uplink is enabled. Home master servers use other ports like 27500 Port 8080 is for UT Server Admin. In the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 and ServerName to the IP assigned to VersaLink from your ISP.
USENET News Service	143 TCP
VNC, Virtual Network Computing	5500 TCP, 5800 TCP, 5900 TCP
Westwood Online, C&C	4000 TCP/UDP, 1140-1234 TCP/UDP
World Wide Web (HTTP)	80 TCP 443 TCP (SSL) 8008 OR 8080 TCP (PROXY)
XBOX Live	TCP/UDP 88 and 3074
Yahoo Messenger Chat	5000-5001 TCP
Yahoo Messenger Phone	5055 UDP
VPN Protocol	**Comments**
IPSec Encryption	IPSec using AH can not be supported through NAT. IPSec using ESP and L2TP can be supported via an ALG
L2TP	IPSec using ESP and L2TP can be supported via an ALG.
PPTP	Works through NAT.

18. HELP

If you select **Help** from the menu bar, a message from the help screens will be displayed. The type of message displayed depends on the menu that you are viewing. If you are viewing a pop-up screen, click the **help** link in the pop-up screen to obtain help messages.

A

About

This screen provides information about VersaLink.

About	
Model Number	VersaLink manufacturer's model number.
Serial Number	VersaLink manufacturer's serial number.
MAC Address	Ethernet MAC (i.e., hardware) Address of VersaLink.
Software Version	VersaLink application software version number.
Software Model	VersaLink application type.
Description	Description of VersaLink protocol processing application software.
Boot Loader	VersaLinks boot loader version number.

Advanced Home Page

The advanced home page offers the same functionality as the home page but adds the ability to change the connection profile settings defined in VersaLink.

About	
Edit	An “Edit” link is added for each connection profile. Selecting this link will pop up a window that allows the connection profile settings to be changed.
New Connection	The “New Connection” link will pop up a window to allow the creation of a new connection profile.

ATM Loopback

ATM Loopback	
ATM Loopback	This setting enables 0/21 loopback. Westell recommends that you do not change this setting.

B

Backup/Restore

This option allows VersaLink configuration to be backed up to or restored from a secure location in flash. The following options are displayed.

Backup/Restore	
Current becomes Back-up	Selecting this command button will backup the current active configuration to the secure flash location.
Back-up becomes Current	This command button will restore the previously stored configuration from the flash location.
Factory becomes Current	This option will restore VersaLink to the state that it arrived in from the factory.

C

Change Administration Password

VersaLink has an administrator password. This password protects VersaLink from any unauthorized modifications to the configuration setting in VersaLink. The following settings are displayed.

Change Administration Password	
Enter Administration Name	This field specifies the Administrator's name. Only one administrator can be defined.
Enter/Verify Administration Password	This field specifies the password required to enable administrator access. The password must be entered twice to ensure that the password has been entered correctly.

Connection Summary

Connection Summary	
Connection Summary	The connection profile screen displays summary information about VersaLink. The connection state is shown along with the amount of traffic has passed through VersaLink. Each connection profile is listed with its associated usage information.

D

Diagnostics Help

This screen provides tools for diagnosing PPP connection problems. Some tests depend on VersaLink's status and the capabilities exercised by previous tests, which may prevent other types of testing.

Beginning of Diagnostics Help screens

DSL
VersaLink status checks the connection. The following is a list of the possible responses:

DSL	
Up	VersaLink is operating correctly and has obtained synchronization with the opposing DSLAM.
Down	Explanation: VersaLink is operating correctly, but has not synchronized with the opposing DSLAM. Solution: First, check to be sure that the cable connecting VersaLink to the ADSL wall jack is properly connected at both ends. If the cable is properly connected and VersaLink does not synchronize, try another phone cable. Next, wait for VersaLink to train. It can sometimes take as long as two minutes for VersaLink to train. If it still has not come into synchronization, power cycle VersaLink. If you have tried the approach above and VersaLink still does not synchronize, contact your service provider.

PPPoE
The PPPoE status indicates if a PPPoE session is established (i.e., if the PPPoE Discovery procedure has completed). The following is a list of the possible responses:

PPPoE	
Session up	A valid PPPoE session has been detected.
no session	Currently there is no active PPPoE session. A PPP session must be connected from the homepage screen.
initiating session	The connection process for a PPPoE session has been initialized. It can sometimes take a few seconds for the PPPoE Discovery procedure to complete. Wait 10-15 seconds and try again. If the PPPoE Discovery still cannot complete, there may be a configuration issue with your service provider's equipment. Verify your VPI/VCI settings (on the LAN Advanced page) and contact your ISP provider.
Session halted	A successful PPPoE session was halted. A PPP session must be connected from the homepage screen.
passed	A valid PPPoE session was established.
Session failure	A PPPoE session could not be made. There may be a configuration issue with your service provider's equipment. Verify your VPI/VCI settings (on the LAN Advanced page) and contact your provider.

PPP
This field displays the PPP Connection status. A PPPoE or PPPoA session must already be established. The following is a list of the possible responses:

PPP	
Connection up	VersaLink has established a PPP connection.
no connection	There is no PPP connection. A PPP session must be connected from the homepage screen.
initiating connection	The PPP connection process has been initialized.
Connection halted	A successful PPP connection was halted. Solution: A PPP session must be connected from the homepage screen.
Cannot connect	Explanation: A PPP connection could not be made because of a PPPoE session failure.
Authorization failure	The username or password is incorrect. Verify that the username and password your Service Provider issued are entered correctly.
Link control protocol failed	Try re-establishing the session (from the home page). If this doesn't help, there may be a configuration issue or other failure with your provider's equipment. Contact your service provider.

Self Test
The Self Test performs an integrity check of certain internal components of VersaLink. The following is a list of the possible responses:

Self Test	
Success	VersaLink is operating correctly.
Flash Corrupt	Explanation: The self-test process has detected a problem with internal flash memory. Solution: Restart VersaLink. If the error persists, contact your service provider.

PING ISPs' VersaLink
The IP remote VersaLink test performs an IP network check (i.e., an IP Ping) of the Service Provider's VersaLink. This test verifies that VersaLink can exchange IP traffic with an entity on the other side of the DSL line. The following is a list of the possible responses:

PING ISP's VersaLink	
Success	VersaLink has detected an IP remote VersaLink connection.
No Response	Explanation: This message will occur when an IP remote VersaLink does not answer the IP Ping. Solution: This test fails when the provider's VersaLink does not give its IP address to VersaLink during session establishment. Try Pinging another host, using the Ping test near the bottom of the Diagnostic screen. If you are able to Ping any host, or even if you are able to find an IP address for a given host name (try "www.yahoo.com"), then the failure of the "IP Remote VersaLink" test is moot, because the success of the Ping demonstrates that you are getting IP traffic across the DSL line. If the separate Ping fails as well, contact your service provider.
could not test	Explanation: Test could not be executed because of VersaLink status.

DNS
The DNS test issues a request to try to resolve the name of a particular host. The host name is entered in the input box. The following is a list of the possible responses:

DNS	
Success	VersaLink has successfully obtained the resolved address. The IP address is shown below the host name input box
No Response	Explanation: VersaLink has failed to successfully obtain the resolved address. Solution: Determine the IP addresses of your DNS servers (from the home page, click "Edit" and then "Advanced"), and then use the Ping test near the bottom of the Diagnostic screen to try to Ping those addresses. This may provide useful information when you contact your service provider and speak with Technical Support.
Host not found	Explanation: The DNS Server was unable to find an address for the given host name. Solution: That host may no longer be available on the Internet. Try entering a different host name.
No data, enter host name	Explanation: There must be a host name entered in the input box.
could not test	Explanation: Test could not be executed because of VersaLink status.

PING

Select **PING** to check IP continuity to a remote computer either within or beyond the Service Providers network.

Enter either the IP address or the hostname of the remote host computer in the input box to the right of the Test button. If you Ping by name, DNS will be used to look up the appropriate IP address for that name.
The following is a list of the possible responses:

PING	
Success	The Remote Host Computer was detected.
No Response	Explanation: This message will occur when there was no response to the Ping from the remote computer. Solution: Bear in mind that many hosts on the Internet are configured for security reasons to not respond to IP Ping messages. If you get a success from the DNS test using the same host name, chances are your connection is fine, whether you can Ping the named host or not.
No name or address to PING	Explanation: There must be a host name or IP address entered in the input box to allow VersaLink to Ping.
could not test	Explanation: Test could not be executed because of VersaLink status.

End of Diagnostic Help Screens

DHCP Configuration

This screen contains the settings which control how VersaLink interacts with the local devices connected to it. Westell recommends that you do not change these settings. The following settings are displayed.

DHCP	
DHCP Server	Dynamic Host Configuration Protocol (DHCP) is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this is enabled for Private LAN.
DHCP Start Address (If DHCP is enabled)	This setting specifies the start of the IP address pool that the modem uses to assign IP addresses to local devices.
DHCP End Address (If DHCP is enabled)	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DHCP Lease (If DHCP is enabled)	This setting specifies the DHCP lease time.

Diagnostic Log

LOGS	
All	Lists both connection and system logs.
Connection	Lists all events related to connection activity (Any traffic on the Ethernet, or DSL ports).
System	Lists all events related to system activity (Time, Errors, Boot Information, etc.).
Remote Logging	
Remote Logging	Contains the configuration for the diagnostics remote logging. Remote diagnostics logging allows the diagnostics logs to be sent to a machine running a syslog server*. If you want to save the diagnostics logs, remote diagnostics logging should be enabled and the IP address of the syslog server must be configured.
Enable	Enables remote logging of diagnostics logs.
Remote IP Address	The IP address of the syslog server machine to which the diagnostics log are to be sent.
**The syslog server must be configured to isten on udp port 514, which is usually the default port. In order for the logs to be saved to the syslog server, the server should be configured to save the logs to a file. Some of the free syslog servers available on the Internet are kiwisyslog, MT_syslog and 3Csyslog.*	

DNS Configuration

VersaLink has a built-in DNS server. VersaLink has a feature called "Dynamic DNS." When an IP address is assigned, VersaLink will interrogate the new device for a machine name using several well-known networking protocols. Any names learned will dynamically be added to the DNS server's table of local hosts. A static host assignment is needed only if the new device does not support any of the well-known protocols. The following settings are displayed.

DNS Configuration Screen	
Domain Name	The name of your network. This uses the internet standard for delineating domain names.
Static Host Assignment	This table allows the creation and maintenance of manually configured DNS entries.
Dynamic Host Assignment	This table shows the current list of devices that have automatically provided information.

E

Edit Connection Profiles

This screen facilitates the changing of connection profile parameters. The following settings are displayed.

Edit Connection Profiles	
Connection Name	This field is a description of the default connection profile that VersaLink will use. Feel free to use whatever description you desire.
Account ID	Your account ID is supplied by your ISP. This text string uniquely identifies you with your ISP.
Account Password	The Account Password is a key phrase or text string that verifies your identity to the ISP.
Service Profile	VersaLink stores several service profiles. A service profile is a collection of settings for the built-in firewall and NAT. These settings control which applications are enabled to talk through VersaLink. This selection specifies which service profile is used when VersaLink is using this connection.
Manual/Auto/Always ON	These radio buttons specify how this connection profile is used. A manual setting requires that this connection must be manually established through the "homepage" connection button. When this is set to auto, VersaLink will monitor the network traffic and determine when a connection needs to be made. The connection process will happen automatically the "Always ON" selection causes VersaLink to aggressively establish a connection with your ISP. Whenever VersaLink detects that the connection to your ISP is down, it will try to re-establish that connection.
Time Out Enable/Connection Time Out	Selecting this option will enable the disconnect timeout. If this option is enabled VersaLink will monitor the ISP connection for activity. If there is no activity for the timeout period, VersaLink will disconnect from the ISP.
Edit VC Connection	This screen is an advanced screen. Modifying parameters identified on this screen can cause severe disruption of your service. VC stands for "Virtual Connection." A VC identifies a connection through the service provider's ATM network to your ISP. It is not recommended that you change anything on these pages unless explicitly instructed by your service provider.

F

Firewall Log

This screen is an advanced diagnostics screen. It alerts you of noteworthy information sent to your modem from the Internet. One thousand entries can be made, but a maximum of 50 entries are displayed at a time. Once 1000 entries have been logged, the oldest entry is removed to make space for new entries as they occur.

Firewall Log	
Details	This option gives more information about the specific log entry
Page Numbers	This option navigates you to the corresponding range of entries. The most recent entries are always on the highest numbered page.
Clear Log	This option removes all entries from the log.
Print/Savable Format	This option opens a new window that contains a list of all logged packets that can be saved or printed.

Firewall Settings

This screen is an advanced configuration screen. It allows you to set the level of security you wish to have on your local network. All security levels except "None" protect against known Internet attacks and devices that attempt to gain remote access to VersaLink. The following settings are displayed.

Firewall Settings	
High	This security level only allows basic Internet functionality. Only Mail, News, Web, FTP, and IPSEC are allowed. No other traffic is allowed. Another restriction of high security is that it can't be modified by NAT configuration options. With High security, you are guaranteed to only pass the previously mentioned traffic.
Medium	This security level only allows basic Internet functionality by default, just like High security. Medium security, however, allows Customization through NAT configuration, so you can enable the traffic that you want to pass.
Low	The low security setting will allow all traffic except for known attacks. With low security, your Gateway is visible by other computers on the Internet.
Custom	Custom is a very advanced configuration option that allows you to edit the firewall configuration directly. Only the most expert users should try this.
Remote Logging	Contains the configuration for the firewall remote logging. Remote firewall logging allows the firewall logs to b sent to a machine running a syslog server*. If you desire to save the firewall logs, remote firewall logging must be enabled and the IP address of the syslog server must be configured.
Enable	This option enables remote logging of firewall logs.
Remote IP Address	The IP address of the syslog server machine on the local area network to which the firewall logs are to be sent.
**The syslog server must be configured to isten on udp port 514, which is usually the default port. In order for the logs to be saved to the syslog server, the server should be configured to save the logs to a file. Some of the free syslog servers available on the Internet are kiwisyslog, MT_syslog and 3Csyslog.*	

H

Home Page

The home page gives you a quick summary of VersaLink's state. The following settings are displayed.

Home Page	
Connection Overview	The Connection Overview section displays the status of the DSL connection. The DSL must show a state of "**UP**" to allow VersaLink to communicate with your service provider's network.
Connection Name	The Connection Name section displays all of the connection profiles that are defined by VersaLink. A connection profile is information that VersaLink needs to establish a connection to your ISP. The "PPP Status" columns will show a status of "**UP**" if VersaLink is currently using that profile to communicate. The command button allows you to control the connection state.
Profile Editor	Selecting the "Profile Editor" link will allow you to define or change any of the connection profile settings.

L

LAN Configuration

This screen contains the setting that controls how VersaLink interacts with the local devices connected to VersaLink. Westell does not recommend that you change these settings. The following settings are displayed.

LAN Configuration	
Gateway IP Address	This controls the IP address that VersaLink uses for local communication.
Subnet Mask	This setting specifies the subnet mask to use to determine if an IP address belongs to your local network.
DHCP Start Address	This setting specifies the start of the IP address pool that VersaLink uses to assign IP addresses to local devices.
DHCP End Address	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DNS Server Enable	DNS stands for Domain Name System. This is an Internet standard that facilitates communication among devices. This allows a name to be used when specifying a device instead of an IP address. Normally you want this enabled.
DHCP Server Enable	DHCP stands for Dynamic Host Configuration Protocol. This is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this opt ion is set to Enabled.

LAN Statistics

This page contains information regarding the configuration and status of your Local LAN. The following settings are displayed.

LAN Configuration	
Device IP Address	This displays the IP address that VersaLink uses for local communication.
DHCP NetMask	This displays the subnet address that VersaLink's DHCP server issues in DHCP responses.
DHCP Start Address	This setting specifies the start of the IP address pool that the modem uses to assign IP addresses to local devices.
DHCP End Address	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DHCP Server Status	Displays the status, "ON" or "OFF" of the DHCP Server
DHCP Server	Displays which network "Public" or "Private" the DHCP server is serving IP addresses for.
Devices on LAN	This page displays the current devices the modem has found on your LAN. The name of the device, the Ethernet MAC address, and the status, "Active" or "Inactive" is displayed in the table.

P

Private LAN

This page contains the settings that control how VersaLink interacts with the local devices connected to VersaLink. It is not recommended that these settings be changed. The following settings are displayed.

Private LAN	
Private LAN DHCP Server Enable	Dynamic Host Configuration Protocol (DHCP) is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this is enabled for Private LAN.
Private LAN Enable	This setting enables the Private NAT'ed interface. It is advised to leave this enabled.
Modem IP Address	This controls the IP address that VersaLink uses for local communication.
Subnet Mask	This setting specifies the subnet mask to use to determine if an IP address belongs to your local network.
DHCP Start Address (If DHCP is enabled for Private LAN)	This setting specifies the start of the IP address pool that the modem uses to assign IP addresses to local devices.
DHCP End Address (If DHCP is enabled for Private LAN)	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DHCP Lease (If DHCP is enabled for Private LAN)	This setting specifies the DHCP lease time.

Protocol

Protocol	
Protocol	This screen informs VersaLink which networking protocol to use when communicating with your ISP. This information is provided by your ISP.

Public LAN

This screen contains the settings that control how VersaLink interacts with the local devices connected to VersaLink. It is not recommended that these settings be changed. The following settings are displayed.

Public LAN	
Public LAN DHCP Server Enable	Dynamic Host Configuration Protocol (DHCP) is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this is enabled for Private LAN.
Public LAN Enable	This setting enables the Public interface. This feature allows a global subnet to exist behind your modem.
Modem IP Address	This controls the IP address that VersaLink uses for local communication.
Subnet Mask	This setting specifies the subnet mask to use to determine if an IP address belongs to your local network.
DHCP Start Address (If DHCP is enabled for Public LAN)	This setting specifies the start of the IP address pool that the modem uses to assign IP addresses to local devices.
DHCP End Address (If DHCP is enabled for Public LAN)	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DHCP Lease (If DHCP is enabled for Public LAN)	This setting specifies the DHCP lease time.

Q

Quality of Service

Quality of Service	
Quality of Service	This feature helps ensure data integrity in high-speed transmissions. This feature provides the capability to partition network traffic into multiple priority levels or classes of service. After packet classification, other QoS features can be utilized to assign the appropriate traffic handling policies including congestion management, bandwidth allocation, and delay bounds for each traffic class.

R

Remote Access

This page allows you to configure your modem so that it can be configured remotely. Once enabled, this feature can be manually disabled, or it will automatically disable after 20 minutes of configuration inactivity.

Remote Access	
Password	This is the password a remote user must enter to access your modem's interface. It must be at least 4 characters long and contain no spaces.
URL	This field contains the URL that must be placed in a remote PC's web browser in order to communicate with your modem. If this field says "Not Connected," you are not currently connected to the Internet.
Enable Remote Access	When you have clicked on this button, entered a valid password, and connected to the Internet, Remote Access will be enabled.
Disable Remote Access	When you have clicked on this button, Remote Access will be disabled.

Routing Information Protocol

Remote Access	
RIP	RIP (Routing Information Protocol) is a widely used protocol for managing VersaLink information within a self-contained network such as a corporate local area network or an interconnected group of such LANs.

S

Single Static IP

This page contains the settings that would allow the PPP address received from the network to be propagated to a single LAN device behind the modem.

Single Static IP	
WAN IP Address	This is the PPP IP address the ISP has assigned the modem.
Selection box	This box contains the devices available to share the Single Static IP address the ISP has assigned the modem. The names listed in the select box will be populated by VersaLink's DHCP server based on DHCP requests. If a device's name cannot be determined, the current IP address of the device will be placed in the list. When the feature is enabled, the active machine will be highlighted in the select box and be displayed at the bottom of the page with the "disable" button. When the feature is disabled, no device in the select box will be highlighted and the "enable" button will be available. When the "User Configured PC" is selected, a local PC must be configured manually with the WAN IP address as its Ethernet adapter's address.

T

Trace Route

The Trace feature allows you to perform an IP trace route to a remote computer either within or beyond the service provider's network. Enter either the IP address or the hostname of the remote host computer into the input box to the right of the Trace button. If you trace by name, DNS will be used to look up the appropriate IP address for that name.

Trace	
Success	Trace will display its progress in the text box. Trace will show three round trip times and the DNS name (if available) of each intermediate VersaLink.
Failure	Trace will display "*" when it does not receive a response or cannot determine the DNS name of an intermediate Gateway. This is not necessarily an error, as some Gateways are configured to ignore trace route packets or do not have DNS name.

Turbo TCP

Turbo
Turbo TCP is a sophisticated network traffic prioritization and queuing method that dramatically improves the performance of downstream TCP/FTP/HTTP transfers under heavy upstream bandwidth utilization conditions. This feature first assigns a high priority to TCP signaling packets in the upstream direction, then places the packet in one of several transmit queues based on this priority. Packets of unspecified priority, like TCP or UDP data, are assigned a low priority and placed in a low priority queue. The packets in the high priority queues are then transmitted before packets in the lower priority queues minimizing any transmit delays. Minimizing the transmit delay of the TCP messages upstream enables the server to send the TCP data downstream faster, resulting in a substantial throughput gain.

U

Update Device

Update Device (Software Upgrade)	
Update Device (Software Upgrade)	This screen is used to upgrade VersaLink's application image. The application image is specified by entering in the filename or by using the browse button.

User Name

This screen is asks for information that will allow VersaLink to make a connection to the ISP on your behalf. VersaLink will need to know your Account ID and Account Password. This information is stored in VersaLink.

User Name	
Connection Name	This is a description of the default connection profile, which VersaLink will use. Feel free to use whatever description you desire.
Account ID	Your Account ID is supplied by your ISP and is a text string that uniquely identifies you with your ISP.
Account Password	The Account Password is a key phrase or text string that verifies your identity to your ISP.

V

VC Configuration

VC Configuration Screen	
VC Configuration	This screen is an advanced screen. Modifying parameters on this screen can cause severe disruption of your service. VC stands for "Virtual Connection." A VC identifies a connection through the service provider's ATM network to your ISP. It is not recommended that anything be changed on these pages unless explicitly instructed by your service provider.

VLAN

VC Configuration Screen	
VLAN	A virtual (or logical) LAN is a local area network with a definition that maps workstations on some other basis than geographic location.

VPI/VCI

VPI/VCI	
VPI/VCI	This screen asks for information that VersaLink needs to establish a communication channel to your ISP. The VPI and VCI values are supplied by your ISP.

W

Wireless Configuration

ACRONYMS	AP-Access Point BSSID-Basic Service Set ID FW-Firmware MAC-Media Access Controller NIC-Network Interface Card PBCC-Packet Binary Convolutional Code SSID-Service Set ID WEP-Wired Equivalent Privacy WLAN-Wireless Local Area Network
Network Name (SSID)	This string, (32 characters or less) is the name associated with the AP (modem). To connect to the AP, the SSID on a Station card must match the SSID on the AP card or be set to "ANY."
Channel	The AP transmits and receives data on this channel. The number of channels to choose from is pre-programmed into the AP card. Station cards do not have to be set to the same channel as the AP; the Stations scan all channels, and look for an AP to connect to.
WEP Security WEP (Wired Equivalent Privacy)	The AP card supports 64-bit, 128-bit, or 256-bit WEP encryption. The WEP option can also be disabled. If so, any station can connect to the modem (as long as its SSID matches the modem's SSID).
text only WEP Key	If selected, the WEP Key is treated as a string of text characters, and the number of characters must be either 5 (for 64-bit encryption) or 13 (for 128-bit encryption) or 29 (for 256-bit encryption). If not selected, the WEP key is treated as a string of hexadecimal characters, and the number of characters must be either 10 (for 64-bit encryption), 26 (for 128-bit encryption), or 58 (for 256-bit encryption). The only allowable hexadecimal characters are 0-9 and A-F. NOTE: The WEP key must be the same value and type for both VersaLink and the wireless network adapter. "Pass Phrase" is not the same as "text" and should not be used.

Enhanced Security	If selected, the SSID is hidden from detection in certain frames of the radio protocol. This makes the SSID harder to discover by external equipment capable of passively scanning the radio signal. Additionally, the station SSID must match the AP Network Name (SSID); the generic station SSID, "ANY" will be refused.
Data Rates (Mbits/s)	These are the allowable communication rates that the AP will attempt to use. The rates are broadcast within the connection protocol as rates supported by the VersaLink. If multiple rates are chosen, multi-rate communication and automatic optimum rate selection is possible. This is the default, and provides the most flexible system. If the Station signal strength or quality is poor, and the throughput of the connection is slow or intermittent, select only the lower two data rates (1 and 2 MB). This can improve performance by reducing the number of pad packets, re-tries and timeouts that could be occurring when the higher rates are automatically trying to be used. Lower rates can be maintained over longer distances and in a wider range of environments.

Wireless Station Configuration

The configuration of wireless stations must correspond with VersaLink's configuration. Typically, WLAN station cards come with a utility for changing the card configuration. Additionally, the WLAN driver might present configuration options as part of the Properties for the installed wireless network adapter. The following configuration items should be considered when setting up a station card.

SSID	This is a description of the default connection profile, which VersaLink will use. Feel free to use whatever description you desire.
Mode	The station's operating mode must be set to, Infrastructure. Most station configuration software will use this term to indicate operation with an AP. Other terms used are ESS or BSS. The terms Ad-Hoc or IBSS indicate operation without an AP; these terms should not be selected.
Tx Rate (Data Rate)	The station's transmission rate (data rate) should be set to Automatic. Selecting a specific data rate is typically only done in difficult environments where conditions limit the maximum possible rate to less than 54 megabits per second.
Encryption	The station's encryption settings must match the AP's settings. This includes the settings for 64-bit, 128-bit, and 256-bit encryption (or none) and the WEP keys. Make certain that the key entries use the same format. The two typical formats provided are simple text entry and hexadecimal entry. Text entry is sometimes termed ASCII entry. **Hexadecimal entry is sometimes termed Hex or Manual entry. Do not use the Pass Phrase option if it is present.**
Authentication Algorithm	On the station, this setting is typically located under the Advanced properties for the wireless network adapter. Two or three algorithm settings are usually present. These might be termed: "Must use Shared for WEP," "Automatic based on WEP setting" and/or "WECA compliant." Select "Automatic based on WEP setting" or "Must use Shared for WEP."

Wireless Statistics

Network Name (SSID)	This string, (32 characters or less) is the name associated with the AP. To connect to the AP, the SSID on a Station card must match the SSID on the AP.
802.11b/g MAC Address (BSSID)	This is the Media Access Controller address of the AP. It is used as the Basic Service Set Identifier.
Primary FW	Primary firmware version number. This is read from the card and helps determine the AP firmware to use. The format of the number is: …>. The version number is also needed to identify existing errata.
Secondary FW	Secondary firmware version number. This is the station firmware that the card would use to operate as a wireless station. The format of the number is …>. The version number is needed to identify existing errata.
OUT and IN	Data preceded by **OUT** pertain to transmissions from VersaLink to a station; VersaLink is the source. Data preceded by **IN** pertain to data received by VersaLink; VersaLink is the destination**.**

OUT-Unicast Frames	The number of successfully transmitted frames whose destination address was a single station, not necessarily the same station, but to any single station: As opposed to a transmission that multiple stations would receive (for example, a broadcast message).
OUT-Multicast Frames	The number of successfully transmitted frames whose destination address was a multicast address (received by more that one station): not necessarily broadcast to all stations, but more than a single station. Broadcast messages are included in the count.
OUT-Fragments	The number of successful transmissions made. This will typically be greater than the sum of the Unicast and Multicast frames because large frames are broken into multiple transmissions. The number of fragments per frame is based on the Fragmentation Threshold setting (not user-configurable).
OUT-Unicast Bytes	The number of bytes transmitted in Unicast Frames, including the header and body of each frame.
OUT-Multicast Bytes	The number of bytes transmitted in Multicast Frames. This includes the header and body of each frame or frame fragment.
OUT-Transmission Deferred	The number of frames (frame fragments) for which one or more transmission attempts were deferred to avoid a collision.
OUT-Frames after single retry	The number of frames that were successfully transmitted after one, and only one, retry. All fragments of the frame must have met this requirement if the frame was fragmented.
OUT-Frames after many retries	The number of frames that successfully transmitted after more than one retry. Any fragment of a frame that required multiple retries would increment this counter for the whole frame.
OUT-Dropped Frames, too many retries	The number of frames that did not transmit due to the short or long retry limit being reached. This number is a result of no acknowledgement or CTS received.
OUT-Discarded Frames	The number of transmit requests that were discarded to free up buffer space. This count is incremented when one of the following occurs: 1) A transmit request is queued too long on the transmit queue due to excessive retries, deferrals, scans, etc. 2) A transmit request is queued too long on the Power-Save queue because the station did not poll or wake up in time.
IN-Unicast Frames	The number of successfully received frames whose destination address was a single location, not necessarily the same location, but to any single location (as opposed to the broadcast address).
IN-Multicast Frames	The number of successfully received frames whose destination address was a multicast address. Broadcast messages are included in this count.
IN-Fragments	The number of fragments successfully received. This might not be equal to the sum of the Unicast and Multicast frames because large frames are broken into multiple transmissions. The number of fragments per frame is based on the Fragmentation Threshold setting (not user-configurable) on the source station.
IN-Unicast Bytes	The number of bytes received in Unicast Frames. This includes the header and body of each frame or frame fragment.
IN-Multicast Bytes	The number of bytes received in Multicast Frames. This includes the header and body of each frame of frame fragment.
IN-Packet not passing checksum	The number of received frames with a Frame Check Sequence (FCS) error.
IN-Drops due to insufficient Rx buffers	The number of received frames discarded due to lack of buffer space.
IN-Un-decryptable packets	The number of received frames (with the WEP sub-field set to one) that were discarded because the frame should not have been encrypted or the source station did not have privacy enabled.
IN-Messages received in message fragments	The number of frames received successfully while another good reception was going on above the carrier detect threshold (the message-in-message path #1 in the modem).
IN-Messages received in bad message fragments	The number of frames received successfully while another reception was going on above the carrier detect threshold, but with a bad or incomplete PLCP Preamble and Header (the message-in-message path #2 in the modem).

19. TECHNICAL SUPPORT INFORMATION

Contact your Internet service provider for technical support.

20. PRODUCT SPECIFICATIONS

ADSL

- DSL Line Code: Discrete Multi-Tone (DMT)
- DSL Rates: 32 kbps to 8 Mbps downstream and 32 kbps to 800 kbps upstream
- Power spectral density: less than -34 dBm/Hz
- DSL Impedance: 100 Ohms
- DSL Performance: per ITU Recommendation G.991.2, ANSI T1.413
- Upgradeable to ADSL2, ADSL2+, READSL

Protocol Features

- Bridge Encapsulation per RFC2684 (Formerly RFC1483)
- Logical Link Control/Subnetwork
- Access Protocol (LLC/SNAP)
- Software Upgradeable
- PPPoE Support
- ATM SAR: Internal to Modem

System Requirements for 10/100 Base-T/Ethernet

- Pentium® or equivalent and above machines
- Microsoft Windows (98 SE, ME, 2000, NT 4.0, or XP) Macintosh OS X, or Linux installed
- Operating system CD
- Internet Explorer 4.x or Netscape Navigator 4.x or higher
- 64 MB RAM (128 MB recommended)
- Ethernet 10/100 Base-T interface
- 10 MB of free hard drive space
- TCP/IP Protocol stack installed

System Requirements for Wireless

- Pentium® or equivalent and above class machines
- Microsoft® Windows® (98 SE, ME, 2000, or XP) or Macintosh® OS X installed
- Operating System CD on hand
- Internet Explorer 4.x or Netscape Navigator 4.x or higher
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- IEEE 802.11b/g PC adapter

LEDs

- Power
- Ethernet (E1, E2, E3, E4)
- Wireless
- DSL
- Internet

Connectors

- DSL: RJ-11, 6-pin modular jack-DSL
- Four Ethernet: 8-pin RJ-45 modular jack (When using the optional uplink jack, ETHERNET1, LAN connection is limited to jacks E2, E3, and E4)
- Power: Barrel connector
- Wireless IEEE 802.11b/g SMA connector and antenna

Power

- Power Supply: External 120 VAC to 12V DC wall-mount power supply
- Power Consumption: Less than 6 watts typical, from 120 VAC

Environmental

- Ambient Operating Temperature: +32 to +104°F (0 to +40°C)
- Relative Humidity: 5 to 95%, non-condensing

EMC/Safety/Regulatory Certifications

- EMC: FCC Part 15, Class B
- UL Standard 60950, 3rd Edition
- CAN/CSA Standard C22.2 No. 60950
- UL
- CSA
- ACTA 968-A
- Industry Canada CS03

21. SOFTWARE LICENSE AGREEMENT

READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY. THIS SOFTWARE IS COPYRIGHTED AND LICENSED (NOT SOLD). BY INSTALLING AND OPERATING THIS PRODUCT, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE SOFTWARE AND HARDWARE TO WESTELL TECHNOLOGIES, INC. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE SOFTWARE BETWEEN YOU AND WESTELL TECHNOLOGIES, INC. (REFERRED TO AS "LICENSOR"), AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES.

1. License Grant. Licensor hereby grants to you, and you accept, a nonexclusive license to use the Compact Disk (CD) and the computer programs contained therein in machine-readable, object code form only (collectively referred to as the "SOFTWARE"), and the accompanying User Documentation, only as authorized in this License Agreement. The SOFTWARE may be used only in connection with the number of systems for which you have paid license fees as dictated in your support agreement. You agree that you will not assign, sublicense, transfer, pledge, lease, rent, or share your rights under this License Agreement. You agree that you may not nor allow others to reverse assemble, reverse compile, or otherwise translate the SOFTWARE.

You may retain the SOFTWARE CD for backup purposes only. In addition, you may make one copy of the SOFTWARE in any storage medium for backup purposes only. You may make one copy of the User's Manual for backup purposes only. Any such copies of the SOFTWARE or the User's Manual shall include Licensor's copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the SOFTWARE or any portions thereof may be made by you or any person under your authority or control.

2. Licensor's Rights. You acknowledge and agree that the SOFTWARE and the User's Manual are proprietary products of Licensor protected under U.S. copyright law. You further acknowledge and agree that all right, title, and interest in and to the SOFTWARE, including associated intellectual property rights, are and shall remain with Licensor. This License Agreement does not convey to you an interest in or to the SOFTWARE, but only a limited right of use revocable in accordance with the terms of this License Agreement.

3. License Fees. The fees paid by you under the support agreement are paid in consideration of the licenses granted under this License Agreement.

4. Term. This License Agreement is effective upon your opening of this package and shall continue until terminated. You may terminate this License Agreement at any time by returning the SOFTWARE and all copies thereof and extracts there from to Licensor. Licensor may terminate this License Agreement upon the breach by you of any term hereof. Upon such termination by Licensor, you agree to return to Licensor the SOFTWARE and all copies and portions thereof.

5. Limitation of Liability. Licensor's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the license fee paid to Licensor for the use of the SOFTWARE. In no event shall Licensor be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if Licensor has been advised of the possibility of such damages. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

6. Governing Law. This License Agreement shall be construed and governed in accordance with the laws of the State of Illinois. You submit to the jurisdiction of the state and federal courts of the state of Illinois and agree that venue is proper in those courts with regard to any litigation arising under this Agreement.

7. Costs of Litigation. If any action is brought by either party to this License Agreement against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorney fees and expenses of litigation.

8. Severability. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof.

9. No Waiver. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

22. PUBLICATION INFORMATION

Westell® VersaLink™ Gateway (Model B90-327W15-06)
Document Part Number 030-300444 Rev. A
December 2005

© 2005 Westell, Inc.
All rights reserved.

Westell, Inc.
750 North Commons Drive
Aurora, Illinois 60504 USA
www.westell.com

All trademarks and registered trademarks are the property of their respective owners.

POWERED BY WindRiver SOFTWARE